PEMBUATAN *INFORMATION SECURITY MANAGEMENT* LAYANAN TEKNOLOGI INFORMASI PADA PPTI STIKOM SURABAYA MENGGUNAKAN ITIL VERSI 3

TUGAS AKHIR

Program Studi

S1 Sistem Informasi

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Oleh:

QURRATUL AINI RACHMAN

13410100080

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

2017

PEMBUATAN *INFORMATION SECURITY MANAGEMENT* LAYANAN TEKNOLOGI INFORMASI PADA PPTI STIKOM SURABAYA MENGGUNAKAN ITIL VERSI 3

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk menyelesaikan
Program Sarjana

Oleh :

Nama : Qurratul Aini Rachman
NIM : 13.41010.0080
Program : S1 (Strata Satu)
Jurusan : Sistem Informasi

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

FAKULTAS TEKNOLOGI DAN INFORMATIKA
INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA
2017

Jika kamu menyerah itulah saat dimana permainan berakhir, karena kemungkinan terbesar adalah memperbesar kemungkinan pada ruang ketidakmungkinan.
(Unknown)

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Kupersembahkan kepada
Seluruh keluarga besar, teman, dan kerabat tercinta

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

TUGAS AKHIR

PEMBUATAN *INFORMATION SECURITY MANAGEMENT* LAYANAN TEKNOLOGI INFORMASI PADA PPTI STIKOM SURABAYA MENGGUNAKAN ITIL VERSI 3

dipersiapkan dan disusun oleh

Qurratul Aini Rachman

NIM : 13410100080

Telah diperiksa, diuji, dan disetujui oleh Dewan Penguji

Pada : September 2017

Susunan Dewan Penguji

Pembimbing

I. Dr. Haryanto Tanuwijaya, S.Kom., M.MT
NIDN. 0710036602

II. Erwin Sutomo, S.Kom., M.Eng.
NIDN. 0722057501

Pembahas

I. Pantjawati Sudarmaningtyas, S.Kom., M.Eng.
NIDN. 0712066801

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tugas Akhir ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana

FAKULTAS TEKNOLOGI DAN INFORMATIKA stikom SURABAYA

Dr. Jusak

Dekan Fakultas Teknologi dan Informatika

FAKULTAS TEKNOLOGI DAN INFORMATIKA

INSTITUT BISNIS DAN INFORMATIKA STIKOM SURABAYA

SURAT PERNYATAAN

PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa Institut Bisnis dan Informatika Stikom Surabaya, saya:

Nama	: Qurratul Aini Rachman
NIM	: 13410100080
Program Studi	: S1 Sistem Informasi
Fakultas	: Fakultas Teknologi dan Informatika
Jenis Karya	: Tugas Akhir
Judul Karya	: "PEMBUATAN *INFORMATION SECURITY MANAGEMENT* LAYANAN TEKNOLOGI INFORMASI PADA PPTI STIKOM SURABAYA MENGGUNAKAN ITIL VERSI 3"

Menyatakan dengan sesungguhnya bahwa:

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, saya menyetujui memberikan kepada Institut Bisnis dan Informatika Stikom Surabaya Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalti Free Right)* atas seluruh isi/ sebagian karya ilmiah saya tersebut di atas untuk disimpan, dialihmediakan dan dikelola dalam bentuk pangkalan data *(database)* untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta
2. Karya tersebut di atas adalah karya asli saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya atau pendapat orang lain yang ada dalam karya ilmiah ini adalah semata hanya rujukan yang dicantumkan dalam Daftar Pustaka saya.
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiat pada karya ilmiah ini, maka saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada saya.

Demikian surat pernyataan ini saya buat dengan sebenarnya.

Surabaya, September 2017
Yang menyatakan

METERAI TEMPEL 9FA4BADF936769035 6000 ENAM RIBU RUPIAH

Qurratul Aini Rachman
NIM : 13410100080

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

ABSTRAK

Pengembangan dan Penerapan Teknologi Informasi (PPTI) merupakan salah satu bagian di Institut Bisnis dan Informatika Stikom Surabaya (Stikom Surabaya). Tujuan utama PPTI ialah mengembangkan dan menerapkan teknologi informasi (TI) untuk mendukung jalannya proses bisnis pada Stikom Surabaya. Saat ini PPTI belum memiliki standar pengelolaan *information security management* pada setiap layanan, sehingga muncul ancaman terhadap keamanan informasi dan dapat menyulitkan PPTI dalam melakukan pengelolaan keamanan informasi dan layanan TI yang dimilikinya.

Solusi untuk permasalahan tersebut yaitu, membuat *information security management* layanan TI yang mengacu pada kerangka kerja *Information Technology Infrastructure Library* (ITIL Versi 3) dalam lingkup *service design*.

Pembuatan *information security management* telah menghasilkan sembilan dokumen yang meliputi kebijakan keamanan informasi, dokumen klasifikasi aset, dokumen penilaian risiko, dokumen insiden keamanan, dokumen tinjauan keamanan, dan dokumen *Standard Operational Procedure* (SOP) yang terdiri dari SOP pengelolaan insiden keamanan teknologi informasi, SOP klasifikasi aset, SOP sosialiasi kebijakan keamanan informasi, dan SOP kontrol keamanan. Hasil tersebut dapat digunakan oleh PPTI untuk melakukan pengelolaan ancaman atau insiden keamanan informasi terhadap layanan TI, sehingga dapat dijadikan pedoman dan dokumentasi untuk melakukan evaluasi, mengambil keputusan untuk menentukan tindakan pengelolaan keamanan informasi dan layanan TI.

Kata Kunci: PPTI Stikom Surabaya, *Information Security Management*, ITIL Versi 3.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

KATA PENGANTAR

Puji rasa syukur kehadirat Allah Subhanahu wa ta'ala atas segala nikmat yang diberikan, sehingga penulis bisa menyelesaikan laporan tugas akhir ini yang berjudul: "Pembuatan *Information Security Management* Layanan Teknologi Informasi pada PPTI Stikom Surabaya Menggunakan ITIL Versi 3". Laporan tugas akhir ini disusun guna rangka untuk memenuhi salah satu syarat dalam menempuh Srata 1 di Institut Bisnis dan Informatika Stikom Surabaya, serta juga bertujuan untuk menambah wawasan, ilmu, dan pengalaman dalam bidang STI dengan dunia kerjanya.

Bagi penulis sendiri penyelesaian laporan tugas akhir ini tidak terlepas dari bantuan berbagai pihak yang telah memberikan banyak masukan, nasehat, saran, kritik dan dukungan moril maupun materil kepada penulis. Oleh karena itu, penulis menyampaikan rasa terima kasih kepada:

1. Orang tua dan keluarga tercinta yang selalu memberikan dukungan dan saran kepada saya dalam menyelesaikan laporan tugas akhir ini
2. Bapak Haryanto Tanuwijaya S.Kom., M.MT selaku Dosen pembimbing I yang banyak memberikan masukan dan koreksi yang sangat berguna dalam membantu terselesaikannya laporan tugas akhir ini.
3. Bapak Erwin Sutomo, S.Kom., M.Eng. selaku Dosen pembimbing II yang banyak memberikan masukan dan koreksi yang sangat berguna dalam membantu terselesaikannya laporan tugas akhir ini.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

4. Ibu Pantjawati Sudarmaningtyas, S.Kom., M.Eng. selaku Dosen Pembahas yang selalu memberikan kritik dan saran yang membangun guna untuk menyelesaikan laporan tugas akhir ini.
5. Ibu Sri Suhandiah, S.S., M.M. selaku kepala bagian PPTI beserta staf yang yang berada pada PPTI Stikom Surabaya yang membantu dan telah memberikan data- data yang dibutuhkan penulis dalam rangka menyelesaikan tugas akhir ini.
6. Taradiva, Mourine, dan Danica selaku Tim Tugas Akhir PPTI yang selama proses pengerjaan selalu saling mendukung guna untuk menyelesaikan penyusunan laporan tugas akhir ini.
7. Serta semua pihak yang ikut berkontribusi dalam proses penyelesaian tugas akhir ini yang tidak dapat saya sebutkan namanya.

Semoga Tuhan Yang Maha Esa memberikan imbalan yang setimpal atas segala bantuan yang telah diberikan. Penyusunan tugas akhir ini, penulis menyadari bahwa penulisan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu maka penulis tetap mengharapkan kritik maupun saran yang membangun agar nantinya dapat berguna kedepannya.

Surabaya, September 2017

Penulis

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

DAFTAR ISI

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

DAFTAR GAMBAR

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

DAFTAR TABEL

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

DAFTAR LAMPIRAN

Halaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pengembangan dan Penerapan Teknologi Informasi (PPTI) merupakan salah satu bagian di Institut Bisnis dan Informatika Stikom Surabaya (Stikom Surabaya) yang memilki peran dan tanggung jawab dalam mendukung berlangsungnya proses bisnis dengan melakukan pelayanan Sistem dan Teknologi Informasi (STI) bagi setiap sivitas. Oleh karena itu, di dalam PPTI terdapat tiga bagian yang memiliki peran masing-masing mulai dari bagian pengembangan infrastruktur jaringan, pengembangan sistem informasi, dan manajemen *website*.

Tujuan utama PPTI Stikom Surabaya ialah mengembangkan dan menerapkan teknologi informasi sebagai bagian yang tak terpisahkan dalam proses pembelajaran dan pelayanan baik akademik maupun non-akademik segenap sivitas Stikom Surabaya. Dalam proses mencapai tujuan PPTI haruslah memiliki perencanaan keamanan informasi. Keamanan informasi merupakan proses manajemen kerangka tata kelola perusahaan dalam menyediakan arah strategis untuk kegiatan keamanan (Hunnebeck dkk, 2011).

Saat ini PPTI Stikom Surabaya belum memiliki standar *information security management* terhadap aset atau sumber daya setiap layanan, sehingga akan menyebabkan munculnya ancaman seperti pencurian data, sabotase, kejadian alam, pelanggaran hak cipta, kegagalan *hardware* dan *software, malware* dan *human error* (Whiteman dkk, 2014). Contoh kasus yang sering terjadi di PPTI Stikom Surabaya adalah adanya kegagalan *hardware* dan *software* seperti kerusakan pada *hardisk* dan sistem operasi yang tidak dapat beroperasi dengan

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

baik yang dapat menghentikan atau melumpuhkaan kinerja *server* atau layanan, sehingga layanan

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

informasi tidak tersedia kepada pengguna (*Availability).* Hal yang dilakukan oleh PPTI untuk meminimalisir dampak yang berkepanjangan dari kasus tersebut adalah dengan mematikan atau menghentikan sementara *service* untuk melakukan pengecekan terhadap sumber kerusakan secara maksimal dan melakukan pemulihan. Selain itu, adanya serangan *malware* pada layanan *website* yang dikelola oleh PPTI dengan merusak konten layanan informasi, sehingga dapat mengganggu keutuhan informasi (*Integrity).* Pada kasus ini, penanganan yang dilakukan PPTI adalah melakukan identifikasi terhadap sumber yang rusak dan melakukan perbaikan dengan cara membersihkan dan mengganti dengan hasil *back-up*. Contoh kasus lain adanya penggunaan data *dummy* membutuhkan akses data pelanggan yang bersifat rahasia ketika menerima keluhan dari pelanggan mengenai ketidakstabilan atau laporan mengenai suatu layanan yang tidak berfungsi, sehingga pada saat melakukan pengecekan untuk pemulihan atau perbaikan tidak memiliki prosedur yang terdokumentasi (*Confidentiality*). Selain itu, adanya ketidakpatuhan terhadap prosedur yang tidak mengkomunikasikan adanya perubahan kepengurusan, sehingga terjadinya penggunaan *user password* yang tidak terdokumentasi oleh orang yang bukan bagian dari PPTI atau pengurus organisasi mahasiswa yang dapat menggunakan layanan tanpa sepengetahuan pihak yang bertanggung jawab (*Authenticity and non-repudiation*).

Untuk bisa mengatasi masalah-masalah tersebut dan menghindari dampak dari masalah tersebut, perlu adanya Manajemen Keamanan Informasi yang mengacu pada standar *Information Technology Infrastructure Library* (ITIL) versi 3. Manajemen Keamanan Informasi penting dilakukan karena merupakan bagian dari jaminan layanan, jika keamanan layanan informasi dan pengolahan informasi

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

tidak dapat dipertahankan pada tingkat yang diperlukan oleh bisnis, maka bisnis tidak dapat memberikan nilai kepada konsumen dan utilitas layanan tidak dapat diakses (Hunnebeck dkk, 2011). Penggunaan standar ITIL dikarenakan merupakan *framework* yang memberikan kerangka kerja dan praktik-praktik terbaik dalam mengelola dan memperbaiki kualitas layanan teknologi informasi untuk diterapkan di dalam organisasi (Cartlidge dkk, 2007).

Keluaran dari tugas akhir ini yaitu: 1. Dokumen Kebijakan Keamanan Informasi, 2. Dokumen Klasifikasi Aset, 3. Dokumen Penilaian Risiko, 4. Dokumen Insiden Keamanan, dan 5. Dokumen Tinjauan Keamanan. Selain itu, penelitian ini juga menghasilkan dokumen *Standard Operational Procedure* (SOP) yang meliputi 1. Sosialisasi Kebijakan Keamanan Informasi, 2. Klasifikasi Aset, 3. Kontrol Keamanan, dan 4. Pengelolaan Insiden Keamanan Teknologi Informasi. Diharapkan dengan adanya keluaran tersebut berguna untuk PPTI dalam memberikan tinjauan atau evaluasi terhadap keamanan informasi pada layanan teknologi dan semua kebijakan yang berhubungan dengan manajemen keamanan bisnis dapat dikelola dengan baik.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

1.2 Perumusan Masalah

Berdasarkan latar belakang yang ada, maka perumusan masalah pada tugas akhir ini yaitu bagaimana membuat *Information Security Management* Layanan Teknologi Informasi pada PPTI Stikom Surabaya yang mengacu pada standar ITIL Versi 3?

1.3 Pembatasan Masalah

Adapun batasan masalah yang dibahas dalam pembuatan tugas akhir ini:

1. Proses pembuatan *Information Security Management* difokuskan pada aset utama yang dimiliki bagian PPTI yang meliputi *Sicyca, Stikomapps, Wired Connection, Wireless Connection,* dan *Brilian*.
2. Data yang digunakan adalah data pada tahun 2015 hingga 2016.
3. PPTI mengacu pada kebijakan internet yang telah dibuat sebelumnya.
4. Tidak menghasilkan kebijakan ataupun dokumen yang berhubungan dengan pemasok/*supplier.*
5. Tidak menghasilkan *Security Management Information System* (SMIS).
6. Pembuatan *Information Security Management* menggunakan ITIL Versi 3 pada tahap *service design* atau tahap perencanaan.

1.4 Tujuan Penelitian

Tujuan dalam penelitian ini yaitu membuat *information security management* yang menghasilkan dokumen 1. Dokumen Kebijakan Keamanan Informasi, 2. Dokumen Klasifikasi Aset, 3. Dokumen Penilaian Risiko, 4. Dokumen Insiden Keamanan, dan 5. Dokumen Tinjauan Keamanan. Selain itu, penelitian ini juga menghasilkan dokumen SOP yang meliputi 1. Sosialisasi Kebijakan Keamanan Informasi, 2. Klasifikasi Aset, 3. Kontrol Keamanan, dan 4. Pengelolaan Insiden Keamanan Teknologi Informasi pada PPTI Stikom Surabaya menggunakan panduan ITIL Versi 3.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dengan adanya pembuatan *Information Security Management* adalah sebagai berikut:

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

1. PPTI dapat melakukan evaluasi terhadap keamanan informasi dan pengelolaan risiko ataupun insiden keamanan pada layanan teknologi informasi (TI).
2. Dapat menambah pengetahuan tentang materi *Information Security Management* pada proses *service design* dan memahami bagaimana proses atau aktivitas *Information Security Management* di suatu unit kerja.
3. Dapat digunakan sebagai referensi belajar atau bagian dari pengembangan ilmu pengetahuan di bidang manajemen keamanan informasi.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan laporan tugas akhir ini dibagi menjadi bab-bab dengan rincian sebagai berikut:

BAB I PENDAHULUAN

Dalam bab ini menjelaskan tentang latar belakang, perumusan masalah, pembatasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini dijelaskan landasan-landasan teori yang digunakan untuk membantu penyelesaian penelitian ini yang meliputi penelitian terdahulu, Layanan Teknologi Informasi, *Information Technology Service Management, Information Technology Infrastructure Library, Service Design, Information Security Management, Responsible, Accountable, Consulted and Informed,* Kebijakan Keamanan Informasi, Penilaian Risiko, dan *Standard Operational Procedure.*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

BAB III METODE PENELITIAN

Dalam bab ini dijelaskan tahapan-tahapan yang dikerjakan oleh peneliti dalam penyelesaian tugas akhir ini. Dimulai dari tahap awal yang meliputi studi literatur, wawancara, dan observasi. Tahap pengembangan yang meliputi membuat kebijakan, membuat *standard operational procedure,* menilai risiko dan mengklasifikasikan aset, serta mengelola insiden keamanan dan menjadwalkan kontrol keamanan. Tahap akhir yang meliputi pembahasan penelitian, kesimpulan dan saran, serta pembuatan laporan tugas akhir.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini dijelaskan tentang hasil yang telah diperoleh dari proses analisa data dan informasi untuk menghasilkan dokumen kebijakan keamanan informasi, dokumen klasifikasi aset, dokumen penilaian risiko, dokumen insiden keamanan, dan dokumen penjadwalan kontrol keamanan. Selain itu juga menghasilkan dokumen SOP yang meliputi sosialisasi kebijakan, klasifikasi aset, kontrol keamanan, dan pengelolaan insiden keamanan menggunakan ITIL Versi 3.

BAB V PENUTUP

Dalam bab ini dijelaskan tentang kesimpulan dari pembahasan yang dilakukan oleh peneliti serta saran untuk proses pengembangan penelitian yang telah dibuat.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

BAB II

LANDASAN TEORI

2.1 Penelitian Terdahulu

Penelitian tentang *Service Strategy* telah dilakukan oleh Hodianto (2016), penelitian tersebut bertujuan untuk merancang dokumen manajemen strategi untuk layanan TI yang memuat tentang strategi, taktik, operasional layanan TI, dan kebijakan yang akan diterapkan pada PPTI Stikom Surabaya. Penelitian *Service Strategy* ini telah menghasilkan dokumen profil PPTI, visi misi PPTI, analisis *Strength-Weaknesss-Opportunity-Threat* (SWOT), lima kebutuhan layanan STI, lima strategi layanan, taktik layanan TI dan lima kebijakan layanan TI.

Penelitian tentang *Service Portofolio* telah dilakukan oleh Handoko (2016), penelitian tersebut menghasilkan sebuah dokumen *Service Portofolio* yang di dalamnya terdapat daftar layanan TI berupa *Service Pipeline, Service Catalogue*, dan *Retired Service,* serta cara pengelolaan layanan TI dalam bentuk SOP pada PPTI Stikom Surabaya.

Penelitian tentang *Availability Management* telah dilakukan oleh Pratama (2016), penelitian tersebut bertujuan untuk menghasilkan informasi ketersediaan layanan STI, rencana peningkatan ketersediaan layanan, adanya mekanisme *monitoring*, evaluasi, pengelolaan, dan pelaporan kondisi layanan TI pada PPTI Stikom Surabaya. Penelitian *Availability Management* telah menghasilkan dokumen *Availability Plan,* dokumen standar *Service Availabiliy,* kebijakan *Availability Management*, dan SOP *recovery plan*.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Penelitian *Service Strategy*, *Service Portofolio*, dan *Availability Management* digunakan sebagai masukan pada proses *Information Security Management.*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Service Strategy dibutuhkan sebagai acuan dalam mengelola layanan TI dan kebijakan-kebijakan yang ada di PPTI. *Service Portofolio* sebagai kebutuhan dalam proses mengklasifikasikan aset layanan pada PPTI, dan *Availability Management* dibutuhkan untuk memastikan ketersediaan layanan untuk dilakukan penilaian risiko dan dilakukan pengelolaan keamanannya. Adapun perbedaan dari penelitian terdahulu dengan tugas akhir ini adalah dari segi penyajian data maupun informasi, adanya pembuatan kebijakan keamanan informasi, kategorisasi aset, risiko dan ancaman dilakukan lebih fokus pada aspek keamanan informasi, dan adanya klasifikasi terhadap insiden-insiden apa saja yang terjadi pada lima layanan PPTI, serta prosedur dan jadwal pengelolaannya.

2.2 Layanan Teknologi Informasi

Layanan merupakan sebuah upaya untuk bagaimana memberikan nilai kepada pelanggan dengan memfasilitasi hasil yang dicapai, tanpa melihat dari biaya spesifik dan risiko-risiko. Hasil yang dicapai menggambarkan mengapa pelanggan menggunakan layanan ini. Layanan Teknologi Informasi merupakan sebuah layanan yang disediakan oleh penyedia layanan TI, layanan TI terdiri dari kombinasi teknologi informasi, orang dan proses (Hunnebeck dkk, 2011).

Penerapan yang dilakukan oleh PPTI Stikom Surabaya saat ini telah memiliki 81 layanan yang digunakan untuk mendukung proses bisnis akademik maupun non akademik (Hodianto, 2016). Pengguna layanan TI yang menjadi target yaitu mahasiswa, karyawan, dan dosen. PPTI Stikom Surabaya sebagai penyedia layanan TI saat ini berfokus pada lima layanan utama yang menjadi prioritas proses bisnis. Adapun lima layanan tersebut dapat dijabarkan pada Tabel 2.1.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 2.1. Prioritas Layanan TI Stikom Surabaya
(Sumber: Hodianto, 2016)

No	Layanan TI	Deskripsi Layanan
1	Stikomapps	Merupakan layanan yang digunakan untuk mengakses kegiatan akademik seperti Sicyca dan Brilan, serta kegiatan non akademik seperti *email*, *drive*, *site*, dan lainnya.
2	Sistem Informasi *Cyber Campus* (Sicyca)	Merupakan layanan yang digunakan untuk memberikan informasi kegiatan akademik dan non-akademik kepada mahasiswa, dosen, dan karyawan. Masing-masing pengguna memiliki akses yang berbeda dalam penggunaannya. Mahasiswa memiliki akses untuk jadwal dan administrasi perkuliahan, keuangan, peminjaman buku, dan lainnya. Sedangkan untuk karyawan berhubungan dengan peminjaman sarana, pengecekan absensi, dan lainnya. Dosen memiliki akses yang sama dengan karyawan, namun ada fasilitas akademik untuk perkuliahan dan pengecekan data mahasiswa wali.
3	*Hybrid Learning* Stikom Surabaya (Brilian)	Merupakan layanan yang digunakan untuk proses belajar mengajar, dengan semua informasi perkuliahan seperti materi, tugas, dan ujian mata kuliah disimpan dan diakses menggunakan *Google Apps*.
4	*Wireless Connection*	Merupakan layanan yang digunakan oleh semua sivitas, baik internal maupun eksternal Stikom Surabaya untuk mengakses internet.
5	*Wired Connection*	Merupakan layanan yang digunakan oleh kalangan internal seperti dosen dan karyawan untuk mengakses internet.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Berdasarkan penjelasan dari Tabel 2.1, lima fokus pada layanan utama tersebut menjadi prioritas karena layanan tersebut memiliki dampak atau pengaruh besar bagi PPTI untuk terus bisa melayani kebutuhan penggunanya yaitu mahasiswa, dosen, dan karyawan. Kebutuhan tersebut berhubungan dengan aktivitas utama yang dilakukan sehari-hari di Stikom Surabaya yaitu meliputi proses akademik dan non akademik untuk menunjang proses belajar mengajar, sehingga layanan tersebut menjadi penting karena selalu digunakan dalam proses bisnis yang ada di Stikom Surabaya.

2.3 Information Technology Service Management

Service Management adalah kumpulan kemampuan organisasi khusus yang meliputi proses, aktivitas, fungsi, dan peran yang digunakan untuk membangun struktur organisasi yang tepat, bagaimana memahami dan mengelola layanan yang mereka sediakan, baik dari segi biaya dan risiko-risiko agar dapat benar-benar memfasilitasi apa yang pelanggan inginkan.

Information Technology Service Management (ITSM) adalah suatu pelaksanaan dan pengelolaan layanan TI yang berkualits, sehingga dapat memenuhi kebutuhan bisnis. Secara umum ITSM merupakan metode strategis yang digunakan untuk merancang dan mengelola, serta mendukung kualitas teknologi informasi yang diterapkan dalam sebuah organisasi (Hunnebeck dkk, 2011).

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

2.4 Information Technology Infrastructure Library

Information Technology Infrastructure Library (ITIL) merupakan sebuah pendekatan yang berbentuk standar kerangka kerja yang digunakan dalam bidang TI sebagai bentuk pengukuran dari kinerja organisasi untuk bagaimana menyelaraskan pelayanan TI yang ada dengan kebutuhan bisnis. ITIL juga memberikan gambaran rinci berupa proses-proses untuk secara terus menerus memperbaiki dan memaksimalkan kualitas layanan TI yang dimiliki sesuai dengan kebutuhan bisnis ataupun dari sudut pandang pelanggan (Cartlidge dkk, 2007).

Secara lebih sederhana ITIL merupakan Kerangka kerja yang memuat bagaimana mengelola layanan yang terintegrasi, berbasiskan proses dan praktik-praktik terbaik yang diterapkan di dalam organisasi. ITIL dikembangkan pertama

kali pada tahun 1989 dan 1995 oleh *Her Majesty's Stationery Office* di Inggris atas nama *The Central Communication and Telecommunication Agency* (CCTA). Kemudian setelah tahun 2000 dimunculkan ITIL versi 2, namun dengan semakin tingginya kebutuhan akan nilai IT, orientasi pelanggan, keamananan, dan tata kelola yang semakin meningkat, maka penerapan ITIL Framework ini harus terus dikembangkan dan diperluas. Akhirnya pada tahun 2007 ITIL Versi 3 dimunculkan oleh UK *Office of Government Commerce* (OGC) dengan fitur yang lebih lengkap dan ruang lingkup yang lebih luas daripada ITIL Versi 2.

Service lifecycle dalam ITIL terdiri atas lima fase, yaitu: 1. *Service Strategy*, 2. *Service Design*, 3. *Service Transition*, 4. *Service Operation*, dan 5. *Continual Service Improvement*. *Service lifecycle* tersebut dapat dilihat pada Gambar 2.1.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Gambar 2.1. *Service Lifecycle of ITIL*

(Sumber: OGC, 2007)

Service Strategy adalah fase yang berporos pada bagaimana merencanakan, baik berhubungan dengan strategi atau tujuan organisasi. *Service Design* adalah fase merumuskan apa yang telah disepakati pada tahap sebelumnya. *Service Transisi* merupakan fase pengimplementasian, dan *Service Operation* merupakan fase yang bertumpu pada bagaimana mengelola operasional layanan TI. Fase yang kelima adalah *Continual Service Improvement* digunakan sebagai fase peningkatan pengetahuan dan termasuk mencakup semua fase (Cartlidge dkk, 2007).

2.5 Service Design

Service Design adalah tahap dalam siklus hidup yang merubah persyaratan baru dari strategi layanan menjadi desain untuk mewujudkan tujuan bisnis. *Service Design* juga merupakan fase merumuskan apa yang telah disepakati pada fase sebelumnya yaitu *Service Strategy*. Tujuan dari fase ini untuk memastikan bahwa layanan yang dirancang telah memenuhi perubahan kebutuhan bisnis, baik itu kebutuhan sekarang maupun kebutuhan masa yang akan datang (Hunnebeck dkk, 2011). Berikut ini adalah aktivitas-aktivitas yang mendukung *Service Design* adalah:

1. *Design Coordination*

Tujuan dari proses koordinasi desain adalah memastikan tujuan dan sasaran dari tahap desain layanan terpenuhi, dengan menyediakan dan memelihara satu titik koordinasi dan kontrol untuk semua kegiatan dan proses dalam tahap *service lifecycle.*

2. *Service Catalogue Management*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Aktivitas yang menyediakan sumber informasi seluruh layanan atau katalog layanan yang telah disepakati atau disetujui secara terpusat.

3. *Service Level Management*

Aktivitas memastikan seluruh layanan yang ada dan diterapkan dapat terukur secara konsisten, serta laporan yang dihasilkan telah sesuai dengan kebutuhan bisnis dan pelanggan. Laporan utama dari aktivitas ini berkaitan dengan *Service Level Agreement* (SLA), *Operational Level Agreement* (OLA), dan perjanjian dukungan lainnya yang mendukung pengembangan kualitas layanan.

4. *Availability Management*

Aktivitas yang memastikan bahwa apakah target ketersediaan layanan dalam seluruh area bisnis telah sesuai ataukah melebihi kebutuhan saat ini dan masa yang akan datang.

5. *Capacity Management*

Merupakan aktivitas yang berhubungan dengan pengelolaan kapasitas atau pasokan sumber daya yang disediakan dan kapasitas sumber daya tersebut telah memenuhi permintaan bisnis.

6. *IT Service Continuity Management*

Merupakan aktivitas yang menjaga kelangsungan dari layanan teknologi informasi untuk tetap bertahan hidup memenuhi kelangsungan bisnis secara keseluruhan.

7. *Information Security Management*

Aktivitas yang digunakan untuk menyelaraskan keamanan TI dengan keamanan bisnis, dan memastikan bahwa keamanan dan risiko yang muncul telah diolah secara efektif, dan sumber daya telah dikelola dengan baik.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

8. *Supplier Management*

Merupakan proses memastikan bahwa penyedia dan layanan yang diberikan dapat dikelola untuk mendukung target dan ekspektasi bisnis organisasi.

2.6 Information Security Management

2.6.1 *Information*

Informasi merupakan hasil dari pengolahan data menjadi suatu bentuk yang lebih berguna atau bermanfaat bagi penerimanya yang dapat menggambarkan suatu kejadian-kejadian nyata dan berguna untuk pengambilan keputusan (Jogiyanto, 1999). Secara lebih sederhana, informasi merupakan proses lanjut dari data yang memiliki nilai tambah bagi yang menerimanya.

2.6.2 *Information Security*

Keamanan informasi adalah menjaga informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk menjamin kontiunitas bisnis, meminimalisir kerugian atau risiko pada organisasi bisnis dan memaksimalkan investasi dan kesempatan usaha (ISO, 2005).

Keamanan informasi merupakan kerangka tata kelola perusahaan dalam menyediakan arah strategis untuk kegiatan keamanan dan memastikan tujuan keamanan tercapai (Hunnebeck dkk, 2011). Keamanan informasi diperlukan bagi organisasi untuk menjamin kontiunitas bisnis dengan memberikan pelayanan informasi kepada pengguna sesuai dengan kebutuhan.

2.6.3 *Information Security Management*

Information Security Management (ISM) merupakan sekumpulan proses manajemen dalam suatu organisasi yang bertanggung jawab untuk melakukan

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

pengelolaan terhadap keamanan dan menyediakan arah strategis, yang berguna untuk menyelaraskan keamanan TI dengan keamanan bisnis (Hunnebeck dkk, 2011). Tujuan dari proses ISM adalah untuk memastikan bahwa keamanan informasi dikelola secara efektif dalam semua kegiatan pelayanan dan manajemen pelayanan. Adapun beberapa faktor yang mendukung tujuan keamanan dari proses ISM adalah sebagai berikut.

1. Informasi diamati oleh atau diungkapkan untuk hanya mereka yang memiliki hak untuk tahu – kerahasiaan (*Confidentiality*).
2. Informasi lengkap, akurat dan dilindungi terhadap modifikasi yang tidak sah – integritas (*Integrity*).
3. Informasi tersedia dan dapat digunakan bila diperlukan, dan sistem dapat dengan tepat menyediakan informasi dan dapat menahan serangan atau mencegah kegagalan yang terjadi – ketersediaan (*Availability*).
4. Transaksi bisnis, serta pertukaran informasi, dapat dipercaya - keaslian (*Authenticity*) dan *non-repudiation*.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Berikut ini adalah proses atau aktivitas yang dilakukan dalam pembuatan *Information Security Management* adalah.

1. Memproduksi, me-*review*, dan merevisi *Information Security Policy* dan kebijakan-kebijakan terkait. Pada proses ini akan dilakukan *review* terhadap berbagai macam kebijakan yang telah dibuat, dan memungkinkan untuk dilakukan perubahan dan membuat kebijakan-kebijakan terkait dengan keamanan informasi. Kebijakan-kebijakan tersebut antara lain adalah sebagai berikut.

a. Kebijakan keamanan informasi secara umum, merupakan kebijakan yang memuat tentang pedoman yang menjelaskan cara bertindak terhadap apa yang harus dilakukan dan larangan dalam melakukan keamanan informasi.
b. Kebijakan penggunaan dan penyalahgunaan aset TI, merupakan kebijakan untuk menggunakan aset TI dan kebijakan ketika aset TI disalahgunakan.
c. Kebijakan kontrol akses, kebijakan yang menerangkan tentang kontrol akses pengguna dan kontrol akses yang dimiliki.
d. Kebijakan pengendalian sandi, merupakan kebijakan untuk penggunaan/pengendalian sandi atau *password* pengguna terhadap suatu informasi.
e. Kebijakan pengendalian email, kebijakan yang memuat tentang ketentuan yang harus dipenuhi yang berhubungan dengan penggunaan/pengendalian email.
f. Kebijakan internet, kebijakan yang memuat tentang ketentuan yang harus dipenuhi yang berhubungan dengan penggunaan internet.
g. Kebijakan anti-virus, merupakan kebijakan yang berhubungan dengan penggunaan/jenis anti-virus.
h. Kebijakan klasifikasi informasi, merupakan kebijakan yang digunakan untuk mengelola dan melindungi aset informasi.
i. Kebijakan klasifikasi dokumen, merupakan kebijakan yang memuat tentang kebijakan melakukan klasifikasi dokumen berdasarkan jenis dan penggunaannya.
j. Kebijakan remote akses / jarak jauh, kebijakan yang harus dipenuhi ketika akses terhadap suatu layanan terpisah jarak/keadaan tertentu.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

k. Kebijakan yang berkaitan dengan akses pemasok untuk layanan TI, informasi dan komponen.

l. Kebijakan pelanggaran hak cipta untuk bahan elektronik, merupakan kebijakan terhadap hak cipta atas suatu produk.

m. Kebijakan pembuangan aset, kebijakan yang berhubungan dengan pembuangan aset layanan yang sudah tidak digunakan atau tidak diproduksi.

n. Kebijakan retensi rekaman, kebijakan yang memuat berkas/catatan/rekaman yang sudah tidak digunakan dalam periode waktu yang lama.

2. Mengkomunikasikan, mengimplementasikan dan menegakkan kepatuhan terhadap semua kebijakan keamanan. Pada tahap ini akan dilakukan koordinasi dengan membimbing semua bagian yang ada terkait kebijakan keamanan informasi pada proses sebelumnya.

3. Menilai dan mengakategorikan aset-aset informasi, risiko, dan kelemahan sistem TI. Pada tahap ini akan dilakukan klasifikasi atau kategorisasi terhadap aset-aset informasi berdasarkan jenisnya, risiko, dan kelemahan yang ada.

4. Secara teratur menilai, *review,* dan melaporkan risiko keamanan dan ancaman. Pada tahap ini, diidentifikasi bagaimana cara dalam melakukan penilaian/cara menilai suatu risiko.

5. Mengimplementasikan, me-*review*, merevisi, dan meningkatkan kontrol-kontrol pengukuran keamanan atau standar respon. Pada tahap ini, dilakukan pelaksanaan, melakukan survey, dan merevisi langkah-langkah atau standarisasi bagaimana pengukuran keamanan atau standar respon seperti

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

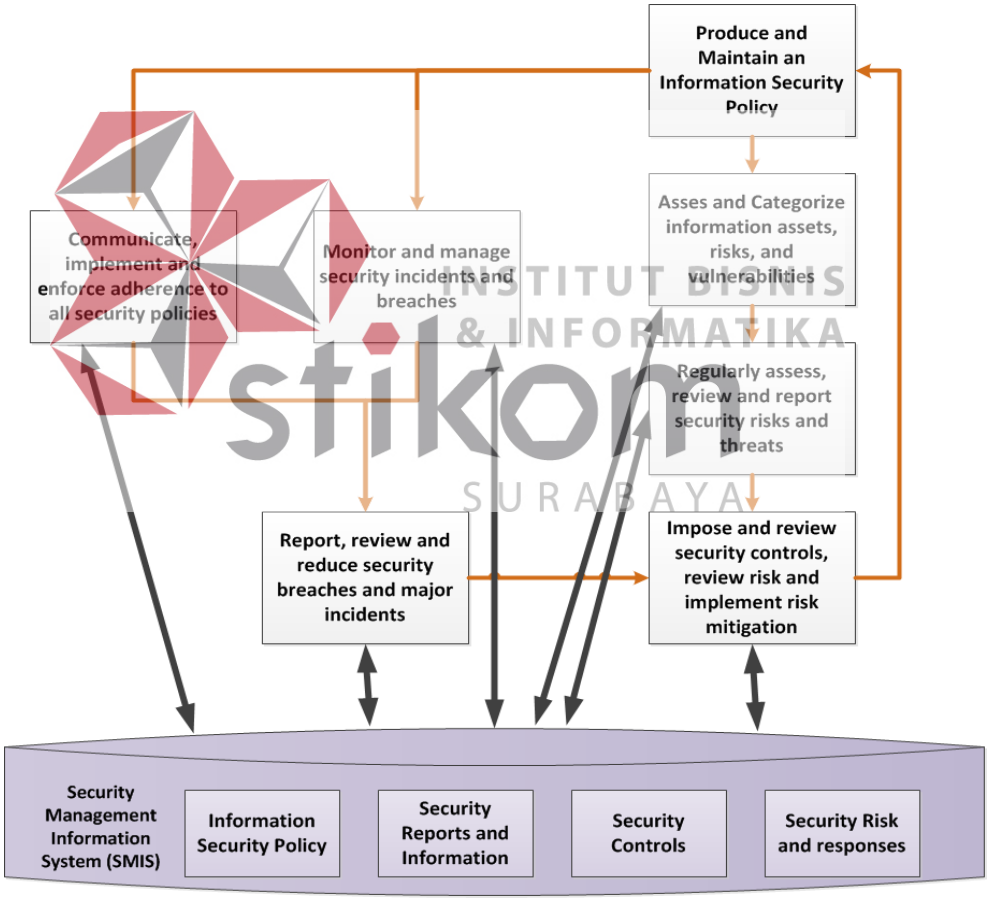
menghindari, pengurangan, pembagian atau penerimaan terhadap risiko keamanan informasi dalam kepentingan bisnis. Adapun kontrol keamanan dapat dilakukan dengan lima cara diantaranya adalah *Preventive, Reductive, Detective, Repressive, and Corrective.*

a. *Preventive*, langkah-langkah keamanan yang digunakan untuk mencegah insiden keamanan yang terjadi. Salah satu contohnya adalah tindakan alokasi hak akses ke kelompok terbatas atau orang yang berwenang.
b. *Reductive*, tindakan untuk mengurangi kerusakan yang disebabkan oleh insiden keamanan, seperti membuat *backup* secara teratur dan pemeliharaan rencana kontingensi.
c. *Detective*, mendeteksi insiden keamanan dengan cepat, seperti melakukan pemantauan terkait dengan prosedur peringatan atau seperti penggunaan perangkat lunak *virus-checking*.
d. *Repressive*, langkah-langkah mencegah kejadian lebih lanjut dengan menangkal setiap pengulangan insiden keamanan yang terjadi. Sebagai contoh, akun atau alamat jaringan sementara diblokir setelah usaha yang gagal untuk *login*.
e. *Corrective*, kerusakan diperbaiki dengan langkah-langkah perbaikan yang sesuai. Misalnya, memulihkan cadangan, atau kembali ke situasi yang stabil sebelumnya (*roll-back*).

6. Memonitor dan mengelola semua pelanggaran keamanan dan insiden-insiden keamanan. Pada tahap ini dilakukan pemantauan dengan melakukan identifikasi terhadap insiden-insiden yang terjadi ataupun pelanggaran lainnya.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

7. Menganalisis, melaporkan, dan mengurangi volume dan dampak dari setiap pelanggaran dan insiden keamanan. Pada tahap ini akan dilakukan analisis dan pemantauan untuk penanganan terhadap insiden-insiden pelanggaran.
8. Menjadwalkan dan menyelesaikan *review* keamanan, audit, dan *penetration test.* Tahap ini berguna untuk melakukan perencanaan/penjadwalan berupa pengontrolan rutin terhadap rencana keamanan yang telah dibuat.Proses atau aktivitas dalam pembuatan *information security management* tersebut dapat dilihat secara lebih detail pada Gambar 2.2.



Gambar 2.2. Aktivitas pada *Information Security Management*

(Sumber: Hunnebeck dkk, 2011)

2.7 Responsible, Accountable, Consulted, Informed

Responsible, Accountable, Consulted, Informed (RACI), fungsi dari RACI adalah untuk menentukkan peran dan tanggung jawab dalam kaitannya dengan suatu aktivitas atau proses tertentu. RACI menyediakan metode yang ringkas dan mudah dalam pelacakan terhadap siapa melakukan apa dalam setiap proses dan memungkinkan suatu keputusan dapat dibuat oleh pihak-pihak yang memang memiliki kewenangan sebagai pembuat keputusan (Hunnebeck dkk, 2011). Berikut ini adalah definisi RACI berdasarkan singkatannya.

R = *Responsible,* pihak atau orang yang bertanggung jawab untuk memastikan proses atau suatu aktivitas telah berhasil dilaksanakan.

A = *Accountable*, pihak atau orang yang memiliki kewenangan untuk menyetujui atau menerima pelaksanaan aktivitas.

C = *Consulted*, pihak atau orang yang pendapatnya dibutuhkan untuk berkonsultasi dalam suatu aktivitas.

I = *Informed*, pihak atau orang yang selalu menjaga kemajuan informasi dengan menerima informasi tentang pelaksanaan proses dan kualitas.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Dalam mendukung kualitas teknologi informasi yang diterapkan dalam sebuah organisasi juga tidak terlepas dari istilah penting seperti *function*, *process* dan *role* (Brewster dkk, 2012).

1. *Function* merupakan sekelompok orang dan alat yang digunakan untuk melaksanakan satu atau lebih proses seperti pelayanan atau operasi TI dan sebagainya.

2. *Process* merupakan seperangkat kegiatan terstruktur yang dirancang untuk mencapai tujuan tertentu. Sebuah proses membutuhkan satu atau beberapa *input* yang didefinisikan dan diubah menjadi sebuah *output.*
3. *Role* merupakan kumpulan tanggung jawab, kegiatan dan otoritas yang diberikan kepada seseorang atau tim. Satu orang atau tim dapat memiliki peran ganda, dan peran juga didefinisikan dalam proses atau fungsi. *Roles* terbagi menjadi dua kategori utama yaitu *generic roles* yang termasuk *process manager* dan *process owner,* serta *specific roles* yang dilibatkan di dalam proses yang termasuk *service design manager,* atau IT *designer. Roles* terbagi menjadi empat sebagai berikut.
   a. *Service Owner*

      Service Owner adalah peran yang bertanggungjawab untuk memastikan bahwa sebuah layanan dikelola dengan fokus bisnis. *Service Owner* bertanggung jawab pada penyampaian layanan TI dan bertanggung jawab kepada *IT Director* untuk penyampaian layanan.

   b. *Process Owner*

      Process Owner bertanggung jawab untuk memastikan bahwa sebuah proses sesuai dengan tujuan. Sebuah proses dipastikan untuk bekerja menurut apa yang disetujui dan didokumentasi dan memenuhi tujuan proses.

   c. *Process Manager*

      Peran *process manager* adalah untuk bertanggung jawab dalam manajemen operasional dari sebuah proses. Salah satu tanggung jawab *Process Manager* adalah memonitor dan melaporkan kinerja proses.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

d. *Process Practitioner*

Process Practitioner bertanggung jawab menjalakan satu atau lebih aktivitas. Selain itu *process practitioner* harus memahami bagaimana peran mereka berkontribusi untuk penyampaian layanan dan membuat nilai untuk bisnis.

2.8 Kebijakan Keamanan Informasi

Menurut Tathagati (2015), Kebijakan merupakan pernyataan resmi organisasi atau perusahaan yang merefleksikan tekad dan komitmen yang dijadikan sebagai landasan utama dan acuan aktivitas organisasi dalam rangka pencapaian visi dan misi organisasi. Kebijakan merupakan dokumen tertinggi yang menyatakan tujuan organisasi atau perusahaan dan komitmen apa yang dilakukan organisasi untuk mencapai tujuan tersebut. Kebijakan organisasi/perusahaan dapat dinyatakan secara umum atau spesifik, bergantung pada kebutuhan perusahaan dalam menyusun sistem tata kerja.

Kebijakan merupakan suatu dokumentasi yang memuat secara resmi tentang harapan manajemen. Kebijakan digunakan untuk mengarahkan keputusan, dan memastikan pengembangan yang konsisten dan tepat dalam pelaksanaan proses, standar, peran, kegiatan, infrastruktur teknologi informasi dan lain-lain. Kebijakan Keamanan Informasi merupakan kebijakan yang mengatur tentang pendekatan organisasi untuk manajemen keamanan informasi, kebijakan keamanan informasi harus memiliki dukungan penuh dan komitmen dari bisnis manajemen eksekutif (Hunnebeck dkk, 2011).

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

2.9 Penilaian Risiko

Penilaian risiko merupakan bagian dari manajemen risiko, penilaian risiko bertujuan untuk mengetahui ancaman-ancaman dari luar yang berpotensi menganggu keamanan informasi organisasi dan potensial kelemahan yang mungkin dimiliki oleh informasi di organisasi (Sarno dan Iffano, 2009). Metode Penilaian Risiko terdiri dari enam tahap yaitu.

1. Identifikasi Aset atau Informasi, melakukan inventarisasi atau pengelompokkan aset ke dalam beberapa kategori atau golongan. Setelah mengidentifikasi aset, kemudian dilakukan penilaian aset. Kriteria nilai aset dapat dilihat pada tabel 2.2.

Tabel 2.2. Kriteria Nilai Aset
(Sumber: Sarno dan Iffano, 2009)

Confidentiality	
Kriteria *Confidentiality*	**Nilai *Confidentiality (NC)***
Public	0
Internal Use Only	1
Private	2
Confidential	3
Secret	4
Integrity	
Kriteria *Integrity*	**Nilai *Integrity (NI)***
No Impact	0
Minor Incident	1
General Disturbance	2
Mayor Disturbance	3
Unacceptable Damage	4
Availability	
Kriteria *Availability*	**Nilai *Availability (NV)***
Low/No Availability	0
Office Hours Availability	1
Strong Availability	2
High Availability	3
Very High Availability	4

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Terdapat tiga kriteria dalam melakukan penilaian terhadap suatu aset, yaitu *Confidentiality, Integrity,* dan *Availability*. Berikut ini merupakan penjelasan dari kriteria tersebut adalah.

1. *Confidentiality,* merupakan kriteria berdasarkan tingkat kerahasiaannya yang meliputi:
   a. *Public,* bebas diakses dan tidak berpotensi mengakibatkan kerugian
   b. *Internal Use Only,* Tidak untuk konsumsi umum luar organisasi dimana penyingkapan akan memengaruhi organisasi/manajemen, tetapi tidak memengaruhi kerugian keuangan atau kerusakan serius pada kredibilitas.
   c. *Private,* data menyangkut informasi personal untuk pemakaian internal.
   d. *Confidential,* data sensitif, digunakan oleh *intern enterprise*. Jika informasi hilang, memberikan efek negatif.
   e. *Secret,* data sangat penting dan memiliki nilai bisnis tinggi.
2. *Integrity,* merupakan kriteria berdasarkan tingkat keutuhannya yang meliputi:
   a. *No Impact,* Tidak ada dampak.
   b. *Minor Incident,* dampak yang ditimbulkan kecil, mengganggu bagian saja.
   c. *General Disturbance,* mengganggu kelancaran kinerja semua Sivitas.
   d. *Mayor Disturbance,* menyebabkan kerugian materi hingga mengurangi reputasi.
   e. *Unacceptable Damage, m*enyebabkan berhentinya proses bisnis hingga konsekuensi hukum.
3. *Availability,* merupakan kriteria berdasarkan tingkat ketersediaannya yang meliputi:

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

a. *Low/No Availability*, ketersediannya <3 jam.

b. *Office Hours Availability*, ketersediaannya 3 - < 8 jam.

c. *Strong Availability*, ketersediaannya 8 - <12 jam.

d. *High Availability*, ketersediaannya 12 - <18 jam.

e. *Very High Availability*, ketersediaannya 18 - < 24 jam.

Berdasarkan Tabel 2.2 untuk menghitung Nilai Aset dapat dilakukan dengan persamaan matematis sebagai berikut:

Nilai Aset (NA) = NC+NI+NV.....(2.1)

Dimana:

NC = Nilai *Confidentiality* sesuai nilai yang dipilih tabel

NI = Nilai *Integrity* sesuai nilai yang dipilih tabel

NV = Nilai *Availability* sesuai nilai yang dipilih tabel

2. Identifikasi Ancaman (*Threat*), ancaman merupakan suatu potensi yang disebabkan oleh insiden yang tidak diinginkan dan mungkin membahayakan proses jalannya bisnis organisasi. Adapun sumber-sumber ancaman dapat berasal dari alam, manusia, dan lingkungan.
3. Identifikasi Kelemahan (*Vulnerability*), kelemahan merupakan kekurangan di dalam prosedur keamanan informasi, perencanaan, implementasi, atau kontrol internal organisasi terhadap penjagaan informasi yang dimiliki, dimana kelemahan ini dapat memicu ancaman.
4. Menentukan kemungkinan ancaman (*Probability*), tujuannya adalah untuk mengetahui kemungkinan jenis ancaman yang akan muncul.

Setelah mengidentifikasi ancaman dan kelemahan, selanjutnya menghitung nilai ancaman (ancaman dan kelemahan) dengan persamaan matematis dengan

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

ketentuan rentang rata-rata nilai probabilitas yang dapat didefinisikan seperti Tabel 2.3.

Tabel 2.3. Skala Probability
(Sumber: Sarno dan Iffano, 2009)

Keterangan *Probability*	**Nilai *Probability***	**Skala Kejadian**
Low	0.1 – 0.3	0 – 3 kejadian
Medium	0.4 – 0.6	4 – 6 kejadian
High	0.7 – 1.0	Lebih dari 6 kejadian

Skala *probability* ditentukkan dengan memberi nilai *probability* yang disesuaikan dengan skala kemungkinan kejadian itu terjadi.

Nilai Ancaman (NT) = ∑PO / ∑Ancaman.....(2.2)

Dimana:

∑PO : Jumlah kemungkinan kejadian

∑Ancaman : Jumalah ancaman terhadap informasi

5. Analisa dampak (*Impact Analysis*), merupakan kegiatan untuk menentukan seberapa besar dampak atau pengaruhnya suatu risiko yang diakibatkan oleh ancaman atau kelemahan terhadap organisasi atau jalannya proses bisnis organisasi. Menentukan skala nilai untuk identifikasi dampak atau yang disebut dengan *Business Impact Analysis (BIA)* dapat dilihat pada Tabel 2.4.

Tabel 2.4. Skala Nilai BIA

Keterangan	**Nilai BIA**	**Nilai Skala**
Low	1	0-12
Medium	2	13-24
High	3	25-36

Keterangan:

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Low : Mengganggu proses bisnis bagian organisasi, menghambat pekerjaan karyawan.

Medium : Mengganggu proses bisnis organisasi, bertambahnya biaya perawatan.

High : Proses bisnis terhenti, menimbulkan kerugian finansial dalam skala besar (biaya pergantian, pendapatan), hingga berpengaruh pada reputasi organisasi.

Rentang Nilai Skala BIA diperoleh dari hasil perkalian nilai tertinggi dari nilai aset, nilai BIA, dan nilai ancaman yang dibagi dengan angka 3, dimana:

Nilai Aset : Nilai terendah adalah 0, nilai tertinggi adalah 12.

Nilai BIA : Nilai terendah adalah 1, nilai tertinggi adalah 3.

Nilai Ancaman : Nilai terendah adalah 0.1, nilai tertinggi adalah 1.0.

6. Menentukan nilai risiko, merupakan gambaran dari seberapa besar akibat yang akan diterima organisasi jika ancaman yang menyebabkann kegagalan keamanan informasi terjadi. Seteleh menentukkan skala BIA dan Risikonya, langkah selanjutnya adalah menilai risiko dengan menggunakan metode matermatis sebagai berikut:

Risk Value = NA x BIA x NT .....(2.3)

Dimana:

NA : Nilai Aset (*Asset Value)*

BIA : Analisa Dampak Bisnis

NT : Nilai Ancaman

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Setelah menentukan nilai risiko, selanjutnya menentukan level risiko dan *treatment* yang dapat diberikan untuk risiko tersebut. Menentukan level dan *treatment* dapat dilihat pada Tabel 2.5.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 2.5. Matriks Level Risiko

Probabilitas Ancaman	**Dampak Bisnis**		
	Low (12)	*Medium* (24)	*High* (36)
Low (0.1)	*Low* 1,2 *Risk Acceptance*	*Low* 2,4 *Risk Acceptance*	*Low* 3,6 *Risk Acceptance*
Medium (0.5)	*Low* 6,0 *Risk Acceptance*	*Medium* 12,0 *Risk Reduction*	*Medium* 18,0 *Risk Reduction*
High (1.0)	*Medium* 12,0 *Risk Reduction*	*High* 24,0 *Risk Avoidance*	*High* 36,0 *Risk Avoidance*

Keterangan:

1. Risiko diterima (*risk acceptance)*

   Organisasi menerima risiko yang terjadi dengan segala dampaknya dan proses bisnis organisasi berlangsung terus.

2. Risiko reduksi (*risk reduction*)

   Organisasi menerima risiko tetapi direduki dengan menggunakan kontrol keamanan sampai pada level yang dapat diterima oleh organisasi.

3. Risiko dihindari atau ditolak (*risk avoidance*)

   Organisasi menghindari risiko yang terjadi dengan cara menghilangkan penyebab timbulnya risiko atau organisasi menghentikan aktvitasnya jika gejala risiko muncul (seperti: mematikan komputer *server*, memutus koneksi jaringan, dan lain-lain).

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

2.10 *Standard Operational Procedure*

Standard Operational Procedure (SOP) secara luas merupakan dokumen yang memuat langkah atau prosedur yang mejabarkan aktivitas operasional yang harus dilakukan secara benar, tepat, dan konsisten di sebuah organisasi. SOP juga dilengkapi dengan formulir dan alur kerja, dan sering digunakan sebagai pedoman untuk mengarahkan dan mengevaluasi suatu pekerjaan. Hasil dari SOP akan menunjukkan konsisten dalam kinerja, produk, berbagai proses pelayanan yang mengacu pada kemudahan pengguna (Tathagati, 2015).

Sedangkan SOP dalam arti sempit sering disebut sebagai prosedur, yang merupakan bagian dari dokumen Sistem Tata Kerja yang mengatur secara rinci aktivitas operasional organisasi agar dapat terlaksana secara sistematis.

2.10.1 Prosedur

Menurut Tathagati (2015), Prosedur adalah dokumen yang lebih jelas dan rinci untuk menjabarkan metode yang digunakan dalam mengimplementasikan dan melaksanakan kebijakan yang telah ditetapkan dalam pedoman. Prosedur merupakan instruksi tertulis sebagai pedoman dalam menyelesaikan sebuah tugas rutin atau tugas yang berulang (repetitif) dengan cara yang efektif dan efisien, untuk menghindari terjadinya variasi atau penyimpangan yang dapat mempengaruhi kinerja organisasi secara keseluruhan. Secara singkat, prosedur menggambarkan strategi yang digunakan untuk memastikan bahwa sebuah proses dilaksanakan dengan baik, konsisten, efektif, dan efisien.

Di Stikom Surabaya, definisi prosedur mengarah pada Standar Pengelolaan Dokumen Sistem Penjaminan Mutu Internal (SPMI) dengan nomor dokumen ST-SM-0.02-002 tanggal 12 oktober Tahun 2015 menjelaskan bahwa

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

standar merupakan dokumentasi tertulis yang berisi berbagai kriteria, ukuran, patokan, atau spesifikasi dari seluruh kegiatan penyelenggaraan pendidikan tinggi di Stikom Surabaya agar dapat dinilai bermutu sesuai dengan ketentuan perundang-undangan, sehingga memuaskan para pemangku kepentingan internal dan eksternal Stikom Surabaya. Berikut ini adalah bentuk *mapping* yang menjelaskan keterkaitan prosedur dan standar dapat dilihat pada Tabel 2.6.

Tabel 2.6. *Mapping* Keterkaitan Prosedur dan Standar

Prosedur	Standar	Keterkaitan
Menurut Tathagati (2015), unsur-unsur yang harus ada prosedur adalah : 1. Judul 2. Penanggung jawab proses 3. Tujuan Prosedur 4. Lingkup aktivitas yang dicakup dalam prosedur tersebut 5. Indikator dan ukuran keberhasilan pelaksanaan proses 6. Definisi istilah 7. Dokumen terkait 8. Siapa yang menyiapkan prosedur 9. Siapa yang memeriksa dan menyetujui/mengesahkan prosedur 10. Tanggal pengesahan	Menurut Standar Pengelolaan Dokumen Sistem Penjaminan Mutu Internal (SPMI) dengan nomor dokumen ST-SM-0.02-002 tanggal 12 oktober Tahun 2015, unsur-unsur yang harus ada pada standar adalah : 1. Siapa yang menyiapkan prosedur 2. Siapa yang memeriksa dan menyetujui/mengesahkan prosedur 3. Tanggal pengesahan 4. Visi dan Misi Organisasi 5. Tujuan dalam membuat prosedur 6. Pihak yang bertanggung jawab 7. Definisi istilah 8. Pernyataan isi standar berisikan aktivitas proses 9. Strategi dalam menjalankan standar 10. Indikator 11. Dokumen Terkait 12. Referensi	Unsur-unsur yang harus ada pada prosedur menurut Tathagati sesuai dengan unsur-unsur yang harus ada pada standar di Stikom Surabaya, sehingga standar pada Stikom Surabaya sama dengan prosedur menurut Tathagati.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

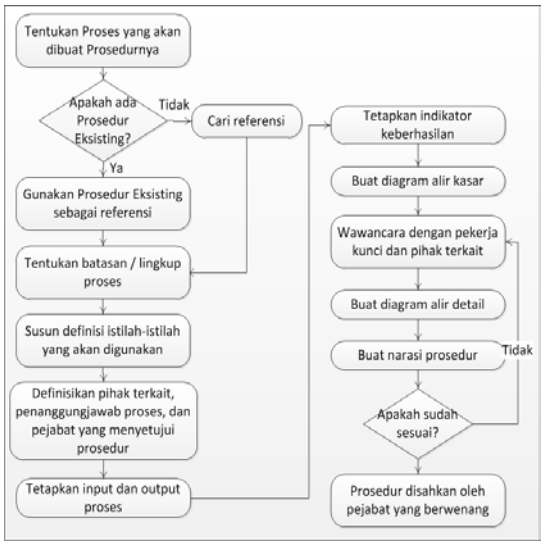
Berikut ini merupakan langkah-langkah penyusunan prosedur yang dapat diuraikan adalah.

1. Periksa apakah sudah ada prosedur eksisting. Jika ada, prosedur eksisting ini bisa dijadikan referensi.
2. Jika organisasi belum memiliki prosedur eksisting, bisa menggunakan referensi prosedur serupa yang diterapkan di organisasi lain. Lebih disarankan untuk menggunakan referensi prosedur dari organisasi atau perusahaan sejenis, agar lebih mudah mendapatkan ekivalensi unit kerja atau individu yang terkait.
3. Tetapkan batasan lingkup proses yang akan dibuatkan prosedur.
4. Definisikan istilah-istilah yang akan digunakan dalam prosedur.
5. Definisikan pihak-pihak yang terlibat dalam proses, fungsi yang bertanggung jawab pada proses, dan pejabat yang berwenang menyetujui Prosedur proses yang akan dibuat.
6. Identifikasikan *input* dan *output* dari proses tersebut dan faktor pengambilan keputusan.
7. Tentukan ukuran keberhasilan dari pelaksanaan prosedur. Indikator keberhasilan bisa berupa jenis, jumlah atau kualitas produk (barang/jasa), atau waktu penyelesaian proses.
8. Buat diagram alir kasar untuk memberikan gambaran proses secara keseluruhan, sebelum menjabarkan proses secara detail.
9. Lakukan wawancara terhadap individu atau unit kerja yang terlibat untuk mengetahui bagaimana pelaksanaan tugas tersebut dilaksanakan secara detail.
10. Buat diagram alir yang lebih rinci sesuai dengan hasil wawancara.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

11. Tuangkan setiap langkah yang telah diidentifikasikan dalam diagram alir dalam bentuk narasi.
12. Apabila dalam aktivitas proses terdapat dokumen lain yang mendukung (misalnya peraturan pemerintah terkait atau formulir terkait), masukan sebagai lampiran.
13. Untuk memastikan apakah prosedur sudah sesuai dengan kondisi yang sebenarnya, gunakan petunjuk-petunjuk sebagai berikut:
    a. Apakah prosedur tersebut sudah cukup jelas?
    b. Apakah urutan langkah dalam Prosedur sudah logis?
    c. Apakah terdapat ide baru yang harus dimasukkan dan dijelaskan?
    d. Apakah kalimat yang menggambarkan setiap langkah mudah dipahami? Apakah kalimatnya terlalu samar? Apakah kalimatnya terlalu panjang dan rumit?
14. Apabila Prosedur sudah dituangkan dalam bentuk tulisan dan diagram alir, Prosedur kemudian diuji coba. Hasil uji coba kemudian digunakan untuk memperbaiki Prosedur hingga sesuai.
15. Setelah Prosedur disahkan, Prosedur didistribusikan kepada unit kerja yang terkait, kemudian dilakukan pelatihan dan sosialisasi.
16. Prosedur sebaiknya ditulis secara singkat, berurutan, dan menggunakan bahasa yang mudah dipahami, serta sebaiknya dilengkapi dengan diagram alir untuk menggambarkan arah proses yang dituangkan dalam Prosedur. Diagram pembuatan prosedur dapat dilihat pada Gambar 2.3.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA



Gambar 2.3. Tahapan Pembuatan Prosedur

2.10.2 Instruksi Kerja

Menurut Tathagati (2015), Instruksi kerja merupakan dokumen yang mengatur secara rinci dan jelas urutan suatu aktivitas yang hanya melibatkan satu fungsi saja sebagai pendukung. Di dalam dokumen instruksi kerja, biasaya merinci langkah demi langkah urutan sebuah aktivitas yang bersifat spesifik atau bersifat teknis.

Di Stikom Surabaya, definisi instruksi kerja mengarah pada pada Standar Pengelolaan Dokumen Sistem Penjaminan Mutu Internal (SPMI) dengan nomor dokumen ST-SM-0.02-002 tanggal 12 oktober Tahun 2015 menjelaskan bahwa prosedur merupakan dokumen tertulis berisi petunjuk pelaksanaan pekerjaan, langkah demi langkah yang mengatur secara rinci setiap kegiatan penyelengaaraan pendidikan tinggi di Stikom Surabaya. Berikut ini adalah bentuk *mapping* yang menjelaskan keterkaitan instruksi kerja dan prosedur dapat dilihat pada Tabel 2.7.

INSTITUT BISNIS & INFORMATIKA Stikom SURABAYA

Tabel 2.7. *Mapping* Keterkaitan Instruksi Kerja dan Prosedur

Instruksi Kerja	Prosedur	Keterkaitan
Menurut Tathagati (2015), instruksi kerja harus memuat unsur-unsur : 1. Lingkup aktivitas 2. Definisi Istilah 3. Penanggung jawab aktivitas 4. Urutan langkah-langkah proses 5. Diagram alir proses 6. Narasi instruksi kerja 7. Pejabat yang menyetujui instruksi kerja	Menurut Standar Pengelolaan Dokumen Sistem Penjaminan Mutu Internal (SPMI) dengan nomor dokumen ST-SM-0.02-002 tanggal 12 oktober Tahun 2015, unsur-unsur yang harus ada pada prosedur adalah : 1. Pejabat yang menyetujui instruksi kerja 2. Tujuan prosedur 3. Ruang Lingkup aktivitas yang dilakukan 4. Definisi istilah 5. Prosedur atau urutan langkah-langkah 6. Kualifikasi pejabat yang menjalankan prosedur 7. Bagan alir prosedur 8. Catatan 9. Referensi	Unsur-unsur yang harus ada pada instruksi kerja menurut Tathagati sesuai dengan unsur-unsur yang harus ada pada prosedur di Stikom Surabaya, karena itu prosedur pada Stikom Surabaya sesuai dengan instruksi kerja menurut Tathagati.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

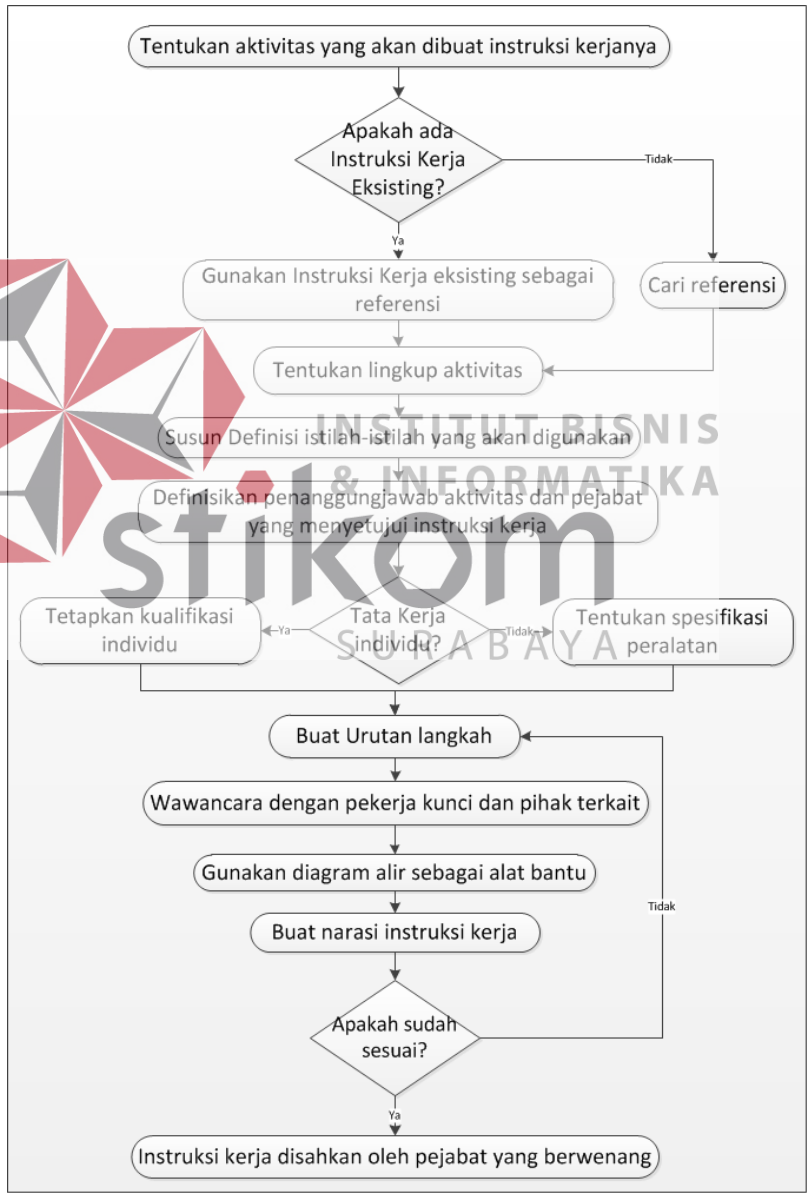
Tahapan pembuatan instruksi kerja dapat dijelaskan sebagai berikut:

1. Periksa apakah pernah ada instruksi kerja eksisting. Jika ada, instruksi kerja tersebut dapat digunakan sebagai referensi.
2. Jika organisasi belum memiliki instruksi kerja bisa menggunakan referensi instruksi kerja serupa yang diterapkan pada organisasi lain.
3. Tetapkan lingkup aktivitas yang akan dibuat instruksi kerja.
4. Definisikan istilah-istilah yang akan digunakan dalam instruksi kerja.

5. Definisikan pihak yang bertanggung jawab dalam aktivitas tersebut dan pejabat yang menyetujui instruksi kerja.
6. Definisikan kualifikasi individu yang akan melaksanakan aktivitas, atau spesifikasi peralatan yang akan dioperasikan.
7. Buat daftar urutan langkah-langkah yang dilakukan dalam pelaksanaan aktivitas atau pengoperasian peralatan.
8. Lakukan wawancara terhadap personel yang terlibat untuk mengetahui bagaimana pelaksanaan tugas tersebut dilaksanakan secara detail.
9. Bila diperlukan, gunakan diagram alir sebagai alat bantu.
10. Tuangkan setiap langkah yang telah diidentifikasi dalam bentuk kalimat perintah.
11. Apabila dalam aktivitas proses terdapat dokumen lain yang mendukung (misalnya peraturan pemerintah, terkait atau form terkait), masukan sebagai lampiran.
12. Untuk memastikan apakah instruksi kerja sudah sesuai dengan kondisi sebenarnya, gunakan petunjuk-petunjuk sebagai berikut:
    a. Apakah instruksi kerja tersebut sudah cukup jelas?
    b. Apakah urutan langkah dalam instruksi kerja sudah logis?
    c. Apakah terdapat ide baru yang harus dimasukan dan dijelaskan?
    d. Apakah kalimat yang menggambarkan setiap langkah mudah dipahami? Apakah kalimatnya terlalu samar? Apakah kalimatnya terlalu panjang dan rumit?

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

13. Apabila Instruksi Kerja sudah dituangkan dalam bentuk tulisan dan diagram alir, Instruksi kerja kemudian diuji coba. Hasil uji coba kemudian digunakan untuk memperbaiki Instruksi kerja hingga sesuai.
14. Setelah Instruksi kerja disahkan, kemudian dilakukan pelatihan dan sosialisasi pada personel terkait. Berikut ini adalah diagram alur pembuatan instruksi kerja yang dapat dilihat pada Gambar 2.4.



Gambar 2.4. Tahapan Instruksi Kerja

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

2.10.3 Rekaman Kerja

Menurut Tathagati (2015), Rekaman adalah bukti bahwa Sistem Tata Kerja yang tertuang dalam pedoman, prosedur, dan instruksi kerja telah dilaksanakan. Rekaman dapat berupa formulir yang telah diisi, lembar kerja yang telah ditandatangani, atau dokumen persetujuan produk yang telah di stempel, dengan tujuan sebagai bukti atau alat telusur berbagai tindakan yang dilakukan dalam melaksanakan sistem tata kerja.

Sesuai dengan prosedur dan instruksi kerja, rekaman berfungsi sebagai dokumentasi bahwa sistem tata kerja telah dilaksanakan serta memudahkan untuk jejak telusur. Jika dalam implementasinya, terdapat pelanggaran dalam prosedur atau instruksi kerja, kondisi ini harus didokumentasikan untuk mengetahui mengapa hal tersebut dilakukan dan siapa yang memberikan izin. Hal ini diperlukan apabila ada investigasi atau temuan audit mengenai pelanggaran tersebut, kejadian tersebut dapat ditelusuri kembali untuk kemudian dilaksanakan evaluasi.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Bentuk-bentuk rekaman dapat berupa formulir yang sudah terisi, lembar kerja yang sudah terisi, daftar, *log book*, grafik, *database*, laporan, notulen rapat, persyaratan perundangan terkait organisasi atau perusahaan, perizinan organisasi atau perusahaan, dan bentuk-bentuk lain yang dapat diterima oleh organisasi sebagai bukti yang sah.

A. Formulir

Salah satu bentuk rekaman yang paling banyak digunakan adalah formulir yang sudah terisi. Formulir merupakan alat bantu berupa lembar yang digunakan dalam melaksanakan sebuah proses atau kegiatan dan mencatat hasilnya sesuai

prosedur atau instruksi kerja. Formulir ini dibutuhkan apabila terdapat kebutuhan pengumpulan atau pencatatan data yang terkait dengan proses organisasi. Formulir ini mempunyai manfaat untuk menunjukkan siapa yang penanggung jawab terjadinya sebuah proses, merekam data proses sebagai bukti bahwa proses telah terjadi atau dilaksanakan, mengurangi kemungkinan kesalahan dalam proses dengan menyatakan semua kejadian dalam bentuk tertulis dan dapat dijadikan bukti apabila terjadi perselisihan atau kesalahan, dan menyampaikan informasi pokok secara tertulis dari satu individu ke individu lain. Langkah-langkah membuat formulir adalah sebagai berikut:

1. Tentukan topik/subjek formulir.
2. Buat daftar informasi apa saja yang diperlukan.
3. Buat pertanyaan yang relevan dengan informasi yang diperlukan.
4. Buat rancangan tata letak formulir dalam kertas kosong.
5. Bila rancangan sudah memenuhi kebutuhan, pindahkan rancangan formulir dalam bentuk formal.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Formulir mengandung informasi yang diperlukan dalam pengendalian dokumen, seperti nomor identifikasi dan nomor revisi/versi, serta tercatat dalam daftar dokumen sistem tata kerja. Sebaliknya, rekaman tidak dikendalikan dengan cara yang sama seperti dokumen sistem tata kerja, melainkan disimpan untuk digunakan sebagai bukti bahwa sistem tata kerja telah terlaksana dengan baik, untuk jejak telusur apabila terjadi kesalahan atau perselisihan, dan analisis data untuk pengembangan sistem tata kerja. Contoh formulir dapat dilihat pada Tabel 2.8.

Tabel 2.8. Contoh Formulir
(Sumber: OGC, 2007)

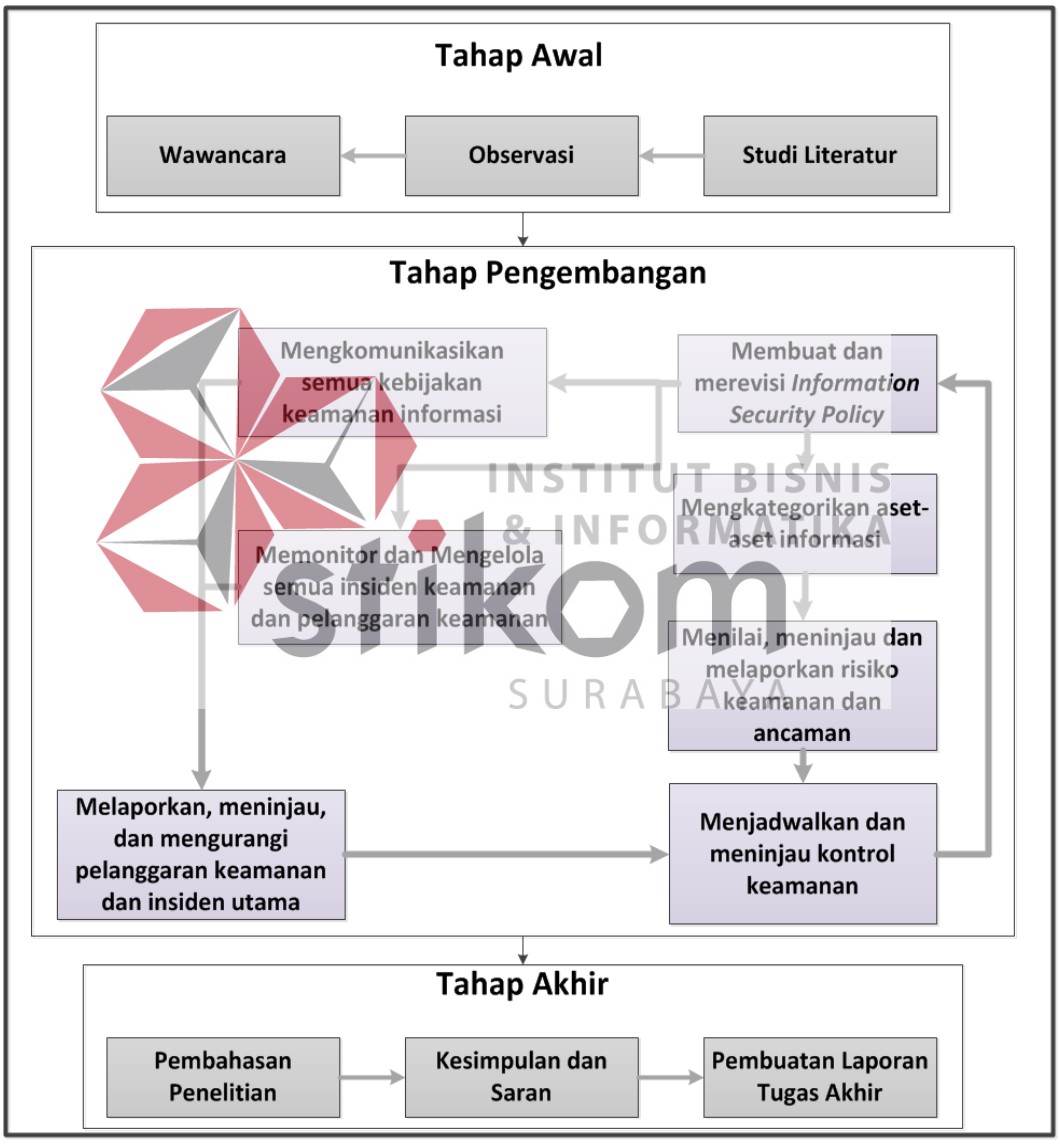
IT Service:	Author:	Date:
Requirement ID:	Requirement Name:	
Source:	Owner:	Priority:
Functional Requirement Description		
Management and Operational and Usability Requirement	Desription:	
Justification:		
Related Document:		
Related Requirement:		
Comments:		
Version No:	Change History:	Change Request:

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

BAB III

METODE PENELITIAN

Penelitian ini terbagi menjadi tiga tahap yaitu: tahap awal, tahap pengembangan, dan tahap akhir. Secara singkat tahapan metode penelitian ini dapat dilihat pada Gambar 3.1.

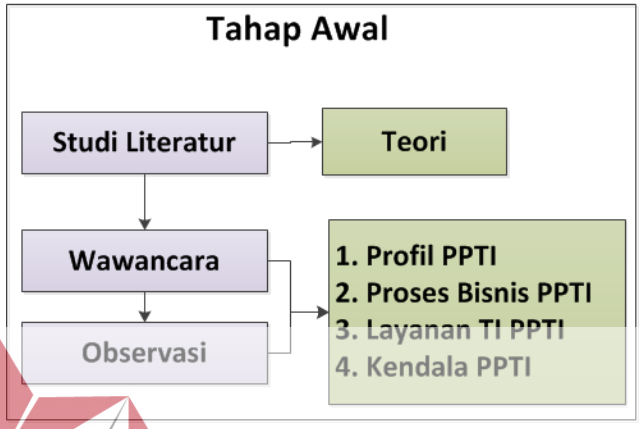


Gambar 3.1. Metode Penelitian Pembuatan *Information Security Management*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.1 Tahap Awal

Pada tahap awal, dilakukan pengumpulan data dan penggalian informasi dilakukan untuk mendapatkan data yang dibutuhkan peneliti dalam menyelesaikan penelitian ini. Pengumpulan data dan penggalian informasi dilakukan dengan tiga tahapan yaitu studi literatur, wawancara, dan melakukan observasi.



Gambar 3.2. Tahap Awal

3.1.1 Studi Literatur

Studi literatur merupakan pendekatan yang digunakan untuk pengumpulan data dalam mendukung tahap pengembangan dan tahap akhir, dengan cara melakukan pengkajian untuk mendapatkan materi lebih mendalam terhadap sumber-sumber tertulis. Literatur yang dibutuhkan adalah berupa buku, jurnal, artikel, referensi laporan tugas akhir dan atau literatur dari internet. Berikut ini literatur yang dibutuhkan yang berhubungan dengan tugas akhir adalah:

1. Layanan TI
2. *ITIL* Versi 3
3. *IT Service Management*
4. *ITIL Service Design*
5. *Information Security Management*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

6. RACI *Chart*
7. Kebijakan Keamanan Informasi
8. Penilaian Risiko
9. Prosedur
10. Instruksi Kerja
11. Rekaman Kerja

3.1.2 Wawancara

Sebelum melakukan wawancara, hal yang harus dilakukan adalah merumuskan pertanyaan-pertanyaan yang berkaitan dengan objek tugas akhir, yang dimana akan dipergunakan sebagai bahan wawancara. Setelah itu, menentukan siapa dan seperti apa narasumber yang dibutuhkan dalam penilitian ini. Untuk menentukkan narasumber yang diwawancara akan menggunakan RACI *Chart* dengan menjabarkan proses atau aktivitas bisnis yang dilakukan, serta peran dan tanggung jawabnya.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Berikut ini adalah *template* yang digunakan dalam menyusun RACI *Chart* dengan menjabarkan deskripsi *organizational development* dapat dilihat pada Tabel 3.1 dan menentukan narasumber yang dibutuhkan dalam penelitian tugas akhir ini dapat dilihat pada Tabel 3.2.

Tabel 3.1. *Template Organizational Development*

Process	Nama Proses
Functions	Nama Fungsi
Roles	*Service Owner:*
	Process Owner:
	Process Manager:
	Process Practitioner:

Tabel 3.2. *Template* RACI *Chart*

Penanggung Jawab / Aktivitas	**Nama Penanggung Jawab**
Aktivitas	

Pada tahap wawancara keluaran yang dapat dihasilkan adalah sebagai berikut.

1. *Organizational development* dan RACI *Chart* yang disajikan dalam bentuk tabel.
2. Visi, Misi dan Tujuan PPTI Stikom Surabaya yang disajikan dalam bentuk tabel.
3. Struktur Organisasi PPTI Stikom Surabaya yang disajikan dalam bentuk Gambar dan Narasi.
4. Kendala-kendala PPTI Stikom Surabaya yang disajikan dalam bentuk daftar atau poin.
5. Layanan teknologi informasi yang menjadi fokus utama PPTI Stikom Surabaya yang disajikan dalam bentuk tabel.

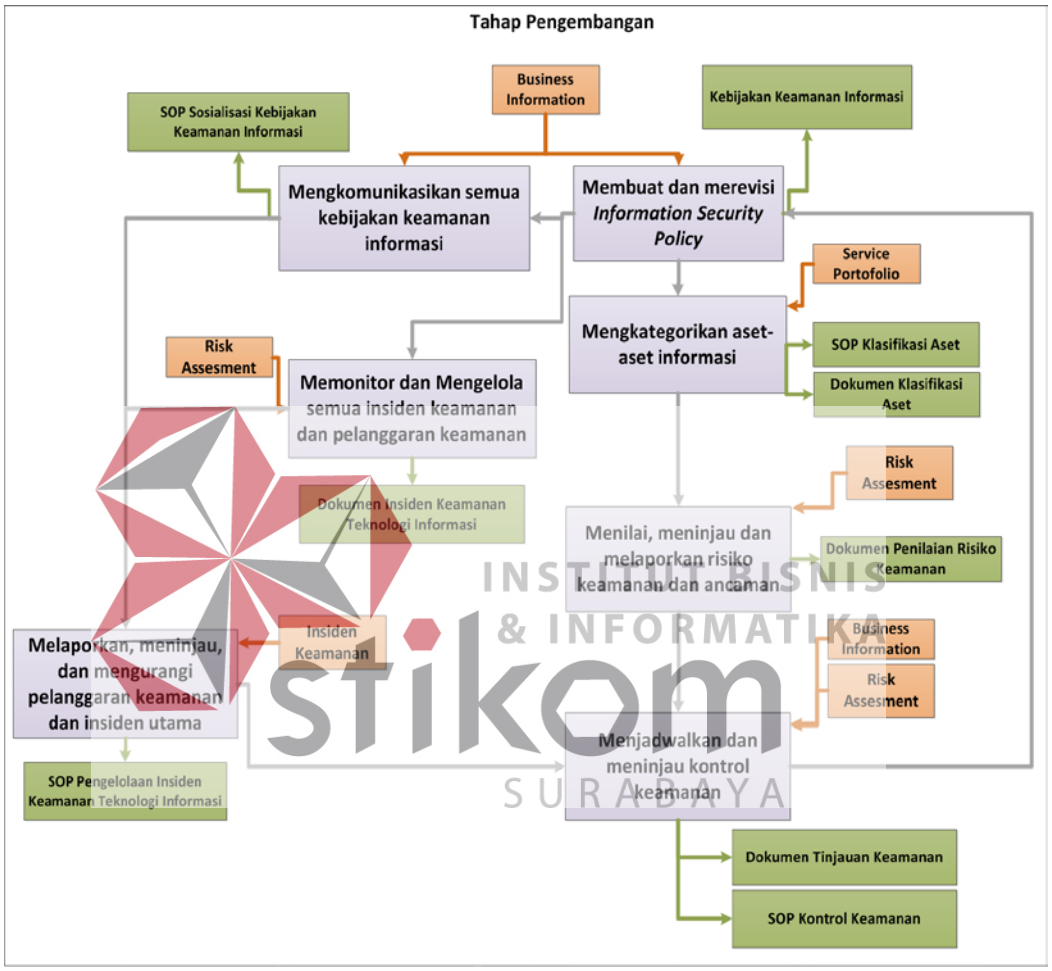
INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.1.3 Observasi

Observasi merupakan metode pengumpulan data yang dilakukan dengan pengamatan secara langsung di lokasi atau tempat kejadian. Pada tahap observasi ini, keluaran yang akan dihasilkan berupa narasi proses bisnis PPTI Stikom Surabaya dan dilengkapi dengan gambar *flowchart*.

3.2 Tahap Pengembangan

Merupakan tahap pengembangan yang dilakukan dalam aktivitas pembuatan *Information Security Management* pada PPTI Stikom Surabaya. Tahap pengembangan tersebut dapat dilihat pada Gambar 3.3.



Gambar 3.3.Tahap Pengembangan

Setiap proses yang dilakukan berdasarkan tahap pengembangan *information security management* akan dibuat *mapping* yang menjelaskan proses pembuatan *information security management* yang ada pada ITIL Versi 3 dan identifikasi kebutuhan sesuai kondisi di PPTI Stikom Surabaya. Setelah itu, akan ditemukan solusi dari penjelasan tersebut yang menjelaskan keluaran yang

dihasilkan dari setiap proses pembuatan *information security management.* Berikut ini adalah *template* dari *mapping* yang dapat dilihat pada Tabel 3.3.

Tabel 3.3. *Template Mapping*

Proses	**ITIL Versi 3**	**PPTI Stikom Surabaya**	**Solusi**
Nama Proses yang dilakukan berdasarkan tahapan pembuatan *information security management*	Identifikasi proses dan kebutuhan ITIL	Identifikasi proses dan kebutuhan PPTI Stikom Surabaya	Solusi yang dibuat berdasarkan hasil identifikasi proses dan kebutuhan ITIL dan PPTI Stikom Surabaya.

Pada pembuatan *information security management,* keluaran *standard operational procedure* (SOP) menggunakan fokus *plan-do-check-act* (PDCA). *Plan* menjelaskan tahap perencanaan apa yang harus dilakukan dan dipersiapkan untuk melakukan sesuatu aktivitas. *Do* menjelaskan tahap penerapan atau melaksanakan semua yang telah direncanakan di tahap *plan. Check* menjelaskan tahap pemeriksaan dan peninjauan ulang serta mempelajari hasil-hasil dari penerapan di tahap *do*. *Action* menjelaskan tahap untuk mengambil tindakan perbaikan atau perubahan terhadap hasil-hasil dari tahap *check.*

3.2.1 Membuat dan merevisi *Information Security Policy*

Pada proses ini akan membuat kebijakan-kebijakan terkait dengan keamanan informasi. Proses ini akan membutuhkan masukan dari informasi bisnis yang diantaranya memuat *template* dan konten yang digunakan untuk pembuatan kebijakan. *Template* yang digunakan dalam membuat dokumen kebijakan keamanan informasi dapat dilihat pada Tabel 3.4.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 3.4. *Template* Kebijakan

1. Objektif	
2. Tujuan Kebijakan	
3. Ruang Lingkup	
4. Deskripsi	
5. Komitmen	
6. Larangan dan Sanksi	

Keluaran yang akan dihasilkan adalah berupa kebijakan keamanan informasi yang di dalamnya meliputi antara lain adalah.

1. Keamanan Informasi Secara Umum
2. Penggunaan dan Penyalahgunaan Aset TI
3. Kontrol akses
4. Kontrol *password*
5. *E-mail*
6. Anti-virus
7. Klasifikasi informasi
8. Klasifikasi dokumen
9. Akses jarak jauh
10. Pelanggaran Hak Cipta untuk Elektronik
11. Penyusutan Aset, dan
12. Retensi *Record*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.2.2 Mengkomunikasikan Semua Kebijakan Keamanan

Pada tahap ini dilakukan proses mengkomunikasikan dalam bentuk sosialiasi, sehingga dokumen yang dihasilkan adalah SOP sosialisasi kebijakan keamanan informasi. Dokumen ini berguna untuk memberikan tata cara dalam melakukan komunikasi atau sosialiasi kepada semua bagian yang berhubungan

dengan kebijakan tersebut. Proses ini akan membutuhkan masukan dari bisnis informasi berupa siapa saja target dalam sosialiasi kebijakan dan *template* yang digunakan. Berikut ini adalah dokumen yang dihasilkan.

1. Standar Sosialisasi Kebijakan Keamanan Informasi, menjelaskan standar melakukan sosialisasi terhadap kebijakan-kebijakan keamanan yang telah dibuat. Berikut ini adalah tampilan desain *template* yang akan digunakan untuk membuat dokumen standar yang dapat dilihat pada Tabel 3.5.

Tabel 3.5. *Template* Standar

1. Visi dan Misi Institut Bisnis dan Informatika Stikom Surabaya	
2. Rasionale	
3. Pihak yang Bertanggung jawab untuk Memenuhi Isi Standar	
4. Definisi Istilah	
5. Pernyataan Isi Standar	
6. Strategi	
7. Indikator	
8. Dokumen terkait	
9. Referensi	

2. Prosedur Sosialisasi Kebijakan Keamanan Informasi, menjelaskan instruksi kerja atau urutan aktivitas kerja sosialisasi kebijakan yang akan dilakukan secara lebih detail. Berikut ini adalah tampilan desain *template* yang akan digunakan untuk membuat dokumen Instruksi Kerja atau Prosedur dapat dilihat pada Tabel 3.6.

Tabel 3.6. *Template* Prosedur

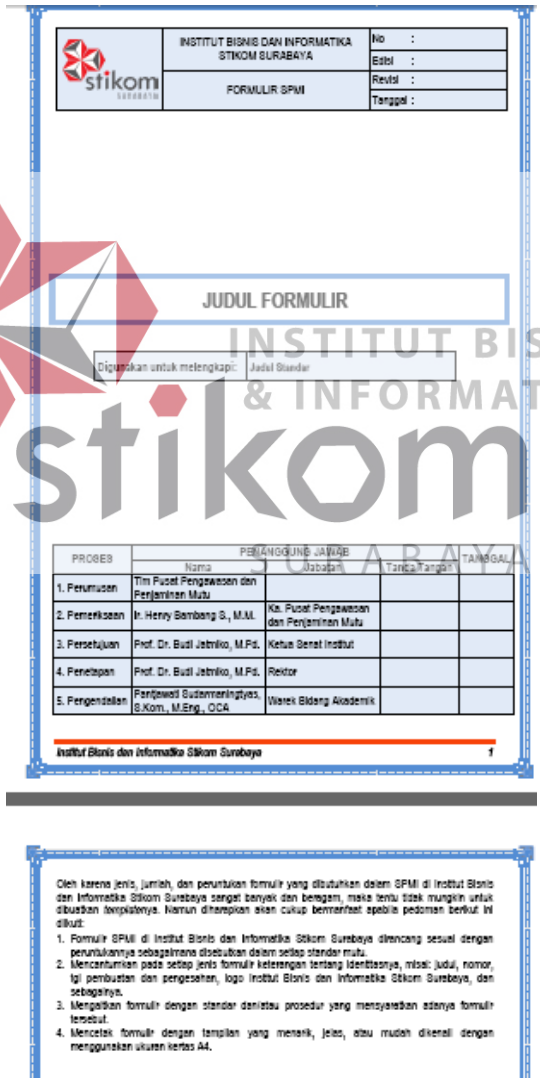
1. Tujuan Prosedur	
2. Luas Lingkup SoP dan Penggunaannya	
3. Standar	
4. Definisi Istilah	
5. Prosedur	
6. Kualifikasi Pejabat/Petugas yang menjalankan SoP	
7. Bagan Alir Prosedur	

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 3.6. (Lanjutan)

8. Catatan	
9. Referensi	

3. Formulir Sosialisasi Kebijakan Keamanan Informasi, bentuk dokumen yang menyatakan hasil atau bukti pelaksanaan kegiatan sosialisasi kebijakan. Berikut ini adalah tampilan desain *template* yang akan digunakan untuk membuat dokumen Rekaman Kerja atau Formulir dapat dilihat pada Gambar 3.4.



Gambar 3.4. *Template* Formulir

3.2.3 Mengakategorikan Aset-Aset Informasi

Pada tahap ini akan menghasilkan dokumen klasifikasi aset, merupakan dokumen lima layanan teknologi informasi yang diklasifikasikan berdasarkan klasifikasi fungsi layanan untuk kebutuhan pengguna dan komponen *tools*, beberapa informasi yang dapat disajikan adalah nama layanan, jenis layanan, pemilik layanan, deskripsi layanan, kelemahan dan kelebihan layanan, fungsi dan komponen layanan, serta rencana pengembangan layanan. Proses ini akan membutuhkan masukan dari *Service Portfolio* yang memuat seluruh layanan yang ada di PPTI. Proses ini juga menghasilkan dokumen SOP Klasifikasi Aset. Berikut ini adalah *template* yang akan digunakan untuk membuat dokumen klasifikasi aset dapat dilihat pada Tabel 3.7 dan Tabel 3.8.

Tabel 3.7. *Template* 1 Dokumen Klasifikasi Aset

Nama Aset		
Jenis Aset		
Pemilik Aset		
Deskripsi Aset		
Kelebihan/Kelemahan Aset		Kelebihan: Kelemahan:
Rencana Pengembangan		
Tools Aset		
No	*Tools*	Kegunaan *Tools*

Tabel 3.8. *Template* 2 Dokumen Klasifikasi Aset

Klasifikasi Aset Berdasarkan Pengguna Layanan		
Pengguna		
Deskripsi Kebutuhan Pengguna		
Fungsi Aset		
No	Fungsi	Deskripsi Fungsi

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.2.4 Menilai, meninjau, dan melaporkan risiko keamanan dan ancaman

Pada tahap ini akan menghasilkan dokumen Penilaian Risiko, pembuatan dokumen ini akan akan melihat data dari penelitian sebelumnya tentang penilaian risiko di dalam dokumen *Availability Management* dan kemudian akan dilakukan pembaharuan atau revisi yang akan disesuaikan dengan proses yang terjadi PPTI. Daftar atau identifikasi risiko akan difokuskan pada lima layanan utama pada PPTI yang telah dijelaskan pada landasan teori. Berikut ini adalah beberapa langkah yang akan dilakukan dalam pembuatan dokumen penilaian risiko adalah.

1. Identifikasi Aset

Berikut ini adalah *template* yang akan digunakan dalam pembuatan identifikasi aset dapat dilihat pada Tabel 3.9.

Tabel 3.9. *Template* Identifikasi Aset

No	Nama Aset	Jenis Pengembangan Aset

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

2. Menghitung Nilai Aset

Nilai aset dapat dihitung dengan menggunakan tiga aspek utama dari keamanan informasi yaitu aspek *Confidentiality*, *Intergrity*, dan *Availability*. Nilai Aset dihitung dengan melakukan persamaan matematis yang dapat dilihat pada rumus 2.1. Berikut ini adalah *template* yang akan digunakan untuk menghitung nilai aset dapat dilihat pada Tabel 3.10.

Tabel 3.10. *Template* Menghitung Nilai Aset

Nama Aset	Kriteria			Nilai Aset (NC+NI+NV)
	Nilai Confidentiality (NC)	Nilai Integrity (NI)	Nilai Availability (NV)	

3. Mengidentifikasi Ancaman dan Kelemahan yang dimiliki oleh aset

Nilai Ancaman (ancaman dan kelemahan) dapat dihitung dengan persamaan matematis yang dapat dilihat pada rumus 2.2. Berikut ini adalah *template* yang akan digunakan dalam mengidentifikasi ancaman dan kelemahan yang dimiliki oleh aset, dapat dilihat pada Tabel 3.11.

Tabel 3.11. *Template* Identifikasi Ancaman dan Kelemahan

Nama Aset			
Jenis Aset			
Risiko	**Jenis Kejadian**	**Probabilitas**	**Rata-rata Probabilitas**
Jumlah Ancaman =	**Jumlah rata-rata probabilitas**		

4. Menentukan Kemungkinan (*Probability*)

Setelah melakukan identifikasi ancaman dan kelemahan, selanjutny adalah menentukan nilai kemungkinan dari ancaman dan kelemahan tersebut. Skala *probability* dapat dilihat pada Tabel 2.3.

5. Analisis Dampak

Dampak analisa bisnis dilakukan dengan menentukan skala nilai *Business Impact Analysis (BIA)* yang dapat dilihat pada Tabel 2.4. Berikut ini adalah *template* yang akan digunakan dalam membuat analisis BIA dapat dilihat pada Tabel 3.12.

Tabel 3.12. *Template* Analisis BIA

No	**Aset**	**Deskripsi BIA**

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

6. Menentukan Nilai Risiko

Langkah selanjutnya adalah menilai risiko tersebut dengan menggunakan metode matermatis berdasarkan rumus 2.3. Setelah nilai risiko diperoleh, selanjutnya menentukan level risiko dan *treatment* yang akan digunakan sesuai dengan matriks level risiko yang dapat dilihat pada Tabel 2.5. Berikut ini adalah *template* menentukan nilai risiko dapat dilihat pada Tabel 3.13.

Tabel 3.13. *Template* Menentukan Nilai Risiko

Aset	**Nilai Aset (NA)**	**BIA**	**Nilai Ancaman (NT)**	**Risk Value**	**Level Risiko**	***Treatment***

3.2.5 Memonitor dan mengelola semua pelanggaran keamanan dan insiden-insiden keamanan.

Pada tahap ini akan membuthkan masukan dari dokumen penilaian risiko untuk di dapatkan pelanggaran-pelanggaran yang terjadi, sehingga menghasilkan dokumen insiden keamanan yang memuat beberapa informasi tentang daftar insiden dan penyebab terjadinya insiden keamanan/pelanggaran yang terjadi dengan fokus pada lima layanan utama di PPTI. Berikut ini adalah *template* yang akan digunakan dalam pembuatan dokumen insiden keamanan dapat dilihat pada Tabel 3.14.

Tabel 3.14 *Template* Insiden Setiap Layanan

Nama Layanan			
Penanggung Jawab			
Deskripsi Insiden			
Insiden	**Penyebab**	**Dampak**	**Alur Pemulihan**

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.2.6 Melaporkan, Meninjau dan Mengurangi Pelanggaran dan Insiden Utama

Pada tahap ini akan membutukan masukan dari dokumen insiden keamanan yang telah dilakukan pada proses sebelumnya, sehingga dapat dibuat prosedur penanganan ketika suatu insiden itu terjadi dengan SOP pengelolaan insiden keamanan teknologi informasi. Berikut ini adalah dokumen yang dihasilkan.

1. Standar Pengelolaan Insiden Keamanan Teknologi Informasi, menjelaskan prosedur bagaimana melakukan pengelolaan terhadap insiden keamanan. *Template* standar dapat dilihat pada Tabel 3.5.
2. Prosedur Pengelolaan Insiden Keamanan Teknologi Informasi, menjelaskan instruksi kerja atau urutan aktivitas kerja pengelolaan insiden keamanan yang akan dilakukan secara lebih detail. *Template* prosedur dapat dilihat pada Tabel 3.6.
3. Formulir Pengelolaan Insiden Keamanan Teknologi Informasi, bentuk dokumen yang menyatakan hasil atau bukti pelaksanaan kegiatan pengelolaan insiden keamanan. *Template* formulir dapat dilihat pada Gambar 3.4.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.2.7 Menjadwalkan dan Meninjau Kontrol Keamanan

Pada tahap ini akan membutuhkan masukan dari bisnis informasi tentang strategi layanan informasi dan dokumen penilaian risiko, sehingga akan menghasilkan dokumen SOP yang memuat tentang langkah-langkah atau standarisasi bagaimana pengukuran keamanan informasi dalam kepentingan bisnis. Berikut ini adalah dokumen yang dihasilkan.

1. Standar Kontrol Keamanan, menjelaskan prosedur bagaimana melakukan kontrol keamanan. *Template* standar dapat dilihat pada Tabel 3.5.

2. Prosedur Kontrol Keamanan, menjelaskan instruksi kerja atau urutan aktivitas kerja kontrol keamanan yang akan dilakukan secara lebih detail. *Template* prosedur dapat dilihat pada Tabel 3.6.
3. Formulir Kontrol Keamanan, bentuk dokumen yang menyatakan hasil atau bukti pelaksanaan kegiatan kontrol keamanan. *Template* formulir dapat dilihat pada Gambar 3.4.

Pada proses ini juga akan menghasilkan sebuah dokumen tinjauan keamanan yang menjelaskan ruang lingkup dan waktu yang harus direncanakan untuk melakukan peninjauan kembali terhadap dokumen atau rencana keamanan. Berikut merupakan *template* yang digunakan dalam pembuatan dokumen tinjauan keamanan dapat dilihat pada Tabel 3.15.

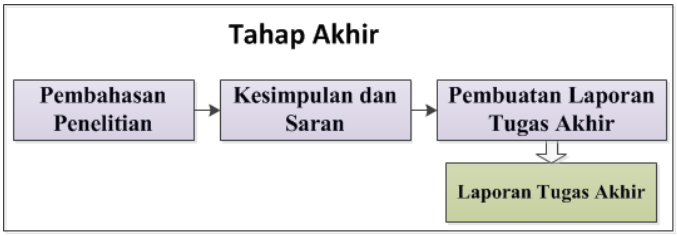
Tabel 3.15. *Template* Dokumen Tinjauan Keamanan

Nama Layanan	
Penanggung Jawab	
Ruang Lingkup	**Tujuan**

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3.3 Tahap Akhir

Tahap Akhir adalah tahap penyelesaian dari tugas akhir ini yang memiliki tiga proses, yaitu:



Gambar 3.5. Tahap Akhir

3.3.1 Pembahasan Penelitian

Pada tahap ini akan dilakukan pembahasan mengenai hasil yang telah diperoleh dari penelitian yang telah dilakukan berdasarkan metode penelitian untuk menghasilkan dokumen atau keluaran dari *information security management.*

3.3.2 Kesimpulan dan Saran

Tahap ini berisi tentang kesimpulan dari pembahasan penelitian yang telah dilakukan dan saran yang akan berguna untuk pengembangan kedepannya.

3.3.3 Pembuatan Laporan Tugas Akhir

Pembuatan laporan tugas akhir akan disusun dalam beberapa bab dan lampiran mengenai seluruh hasil yang telah dilakukan dari penilitian tugas akhir ini.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini membahas hasil dan analisis yang dilakukan dalam proses pembuatan *information security management* layanan teknologi informasi pada PPTI Stikom Surabaya menggunakan ITIL versi 3. Hasil dan analisis tersebut diperoleh dari metode yang digunakan, dimulai dari tahap awal, tahap pengembangan, dan tahap akhir.

4.1 Tahap Awal

Pada tahap ini dilakukan pengumpulan data dan informasi tentang hasil yang mendukung penelitian tugas akhir ini, yang meliputi studi literatur, wawancara, dan observasi.

4.1.1 Studi Literatur

Adapun studi literatur yang mendukung proses pengolahan data dan informasi yang diterima dari PPTI atau yang mendukung pengerjaan laporan tugas akhir ini adalah berkaitan dengan beberapa teori, yaitu.

1. Layanan Teknologi Informasi, suatu upaya untuk bagaimana memberikan nilai kepada pelanggan dengan kombinasi yang dilakukan oleh penyedia layanan seperti teknologi informasi, proses ataupun orang.
2. *ITIL* Versi 3, merupakan sebuah pendekatan yang berbentuk standar kerangka kerja yang digunakan dalam bidang TI sebagai bentuk pengukuran dari kinerja organisasi untuk bagaimana menyelaraskan pelayanan TI yang ada dengan kebutuhan bisnis. ITIL Versi 3 muncul pada tahun 2007 oleh OGC yang menggunakan pendekatan *Service Life Cycle* yang berorientasi bagaimana

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

meningkatkan apa yang dimiliki untuk memastikan penyesuaian terhadap standar baru untuk proses pembaharuan *hardware* dan *software.* ITIL Versi 3 secara tidak langsung telah melakukan revisi terhadap ITIL Versi 1 dan 2, dimana pada Versi 1 lebih fokus pada fungsi internet dan Versi 2 berfokus pada *Service Delivery* dan *Service Support.*

3. *IT Service Management,* merupakan suatu pelaksanaan dan pengelolaan layanan TI yang berkualits, sehingga dapat memenuhi kebutuhan bisnis.
4. *ITIL Service Design,* adalah fase merumuskan apa yang telah disepakati pada fase sebelumnya yaitu *Service Strategy,* dimana siklus yang merubah persyaratan baru dari strategi layanan menjadi desain untuk mewujudkan tujuan bisnis.
5. *Information Security Management,* sekumpulan proses manajemen dalam suatu organisasi yang bertanggung jawab untuk melakukan pengelolaan terhadap keamanan dan menyediakan arah strategis, yang berguna untuk menyelaraskan keamanan TI dengan keamanan bisnis.
6. RACI *Chart,* RACI adalah akronim dari *Responsible, Accountable, Consulted, Informed.* RACI juga menyediakan metode yang ringkas dan mudah dalam pelacakan terhadap siapa melakukan apa dalam setiap proses dan memungkinkan suatu keputusan dapat dibuat oleh pihak-pihak yang memang memiliki kewenangan sebagai pembuat keputusan.
7. Kebijakan Keamanan Informasi, kebijakan merupakan dokumen tertinggi yang menyatakan tujuan organisasi atau perusahaan dan komitmen apa yang dilakukan organisasi untuk mencapai tujuan tersebut atau secara sederhana merupakan suatu dokumentasi yang memuat secara resmi tentang harapan

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

manajemen. Sedangkan Kebijakan Keamanan Informasi merupakan kebijakan yang mengatur tentang pendekatan organisasi yang berhubungan dengan manajemen keamanan suatu informasi.

8. Penilaian Risiko, merupakan suatu teknik yang bertujuan untuk mengetahui ancaman-ancaman dari luar yang berpotensi menganggu keamanan informasi organisasi dan potensial kelemahan yang mungkin dimiliki oleh informasi di dalam organisasi.
9. Prosedur, merupakan dokumen yang lebih jelas dan rinci yang menggambarkan strategi yang digunakan untuk memastikan bahwa sebuah proses dilaksanakan dengan baik, konsisten, efektif, dan efisien.
10. Instruksi Kerja, merupakan dokumen yang mengatur secara rinci dan jelas urutan suatu aktivitas yang hanya melibatkan satu fungsi saja sebagai pendukung.
11. Rekaman Kerja, adalah bukti bahwa Sistem Tata Kerja yang tertuang dalam pedoman, prosedur, dan instruksi kerja telah dilaksanakan.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

4.1.2 Wawancara

Wawancara dilakukan dengan merumuskan pertanyaan-pertanyaan yang berkaitan dengan objek tugas akhir. Dokumen hasil wawancara dapat dilihat pada lampiran 1. Berikut ini adalah beberapa keluaran yang didapatkan dari pelaksanaan wawancara adalah.

A. *Organizational Development*

Organizational development digunakan dalam menentukan narasumber dengan berbagai proses bisnis yang ada di PPTI Stikom Surabaya. Tujuan dari

organizational development adalah untuk menjabarkan *process*, *functions*, dan *roles* yang ada di PPTI Stikom Surabaya.

Process menggambarkan aktivitas yang dilakukan dalam suatu organisasi, *functions* menggambarkan sekelompok orang dan alat yang digunakan untuk melaksanakan satu atau lebih proses, sedangkan *roles* dapat dibagi menjadi empat, yaitu *service owner, process owner. Process manager,* dan *process practitioner*. *Service owner* bertanggung jawab untuk penyampaian layanan teknologi informasi kepada bagian yang berperan. *Process owner* bertanggung jawab pada sebuah proses sesuai dengan tujuan. *Process manager* bertanggung jawab dalam memonitor dan melaporkan kinerja proses. *Process practitioner* bertanggung jawab menjalankan satu atau lebih aktivitas.

Proses *organizational development* yang ada di PPTI Stikom Surabaya terdiri dari empat proses, yaitu proses menyediakan layanan teknologi informasi, proses mengembangan sistem informasi, proses menyediakan informasi, dan proses layanan keluhan. Proses-proses tersebut dapat dilihat pada Tabel 4.1, Tabel 4.2, Tabel 4.3, dan Tabel 4.4. Proses menyediakan layanan teknologi informasi dijalankan oleh tiga fungsi yang ada di PPTI Stikom Surabaya, yaitu Seksie Pengembangan Jaringan, Seksie Pengembangan Sistem Informasi, dan Pengembangan Media *Online. Service owner* untuk proses ini yaitu Diana Fitri, A.Md. Pemetaan *organizational development* untuk proses menyediakan layanan teknologi informasi dapat dilihat pada tabel 4.1.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 4.1. *Organizational Development* Penyedia Layanan

Process	Menyediakan Layanan Teknologi Informasi
Functions	Seksi Pengembangan Jaringan Seksi Pengembangan Aplikasi dan Pengembangan Media *Online*
Roles	***Service Owner**:* Diana Fitri, A.Md.
	***Process Owner**:* Slamet, M.T., CCNA Satria Agung Pamuji Lina Indrawati, S.Kom. Bobby Hartanto Dwi Putra Wijaya, S.Kom. Anita Izathy Chairina, S.Kom. Eva Pramita, S.Kom Rahman Nur Hadi Isnainul Amanda Perwirasari, S.Kom.
	***Process Manager**:* Sri Suhandiah, S.S., M.M Slamet, M.T., CCNA. Lina Indrawati, S.Kom
	***Process Practitioner**:* Slamet, M.T., CCNA Satria Agung Pamuji Lina Indrawati, S.Kom. Bobby Hartanto Dwi Putra Wijaya, S.Kom. Anita Izathy Chairina, S.Kom. Eva Pramita, S.Kom Rahman Nur Hadi Isnainul Amanda Perwirasari, S.Kom.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Pemetaan *organizational development* untuk proses Mengembangkan Sistem Informasi yang Berjalan di Stikom Surabaya dijalankan oleh dua fungsi yang ada di PPTI Stikom Surabaya, yaitu Seksie Pengembangan Jaringan dan Seksie Pengembangan Sistem Informasi. *Service owner* untuk proses ini yaitu Diana Fitri, A.Md. Berikut ini adalah pemetaan *organizational development* mengembangkan sistem informasi yang dapat dilihat pada Tabel 4.2.

Tabel 4.2. *Organizational Development* Sistem Informasi

Process	Mengembangkan Sistem Informasi yang Berjalan di Stikom Surabaya
Functions	Seksi Pengembangan Jaringan Seksi Pengembangan Aplikasi
Roles	***Service Owner**:* Diana Fitri, A.Md.
	***Process Owner**:* Slamet, M.T., CCNA Lina Indrawati, S.Kom.
	***Process Manager**:* Sri Suhandiah, S.S., M.M
	***Process Practitioner**:* Satria Agung Pamuji Bobby Hartanto Dwi Putra Wijaya, S.Kom. Anita Izathy Chairina, S.Kom. Eva Pramita, S.Kom Rahman Nur Hadi

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Proses menyediakan informasi di Stikom Surabaya dijalankan oleh dua fungsi yang ada di PPTI Stikom Surabaya yaitu Seksie Pengembangan Jaringan dan Seksie Pengembangan Sistem Informasi. *Service owner* untuk proses ini yaitu Diana Fitri, A.Md. Pemetaan *organizational developmet* untuk proses menyediakan informasi yang ada di PPTI Stikom Surabaya dapat dilihat pada Tabel 4.3.

Tabel 4.3. *Organizational Development* Penyediaan Informasi

Process	Menyediakan Informasi
Functions	Seksi Pengembangan Jaringan Seksi Pengembangan Aplikasi
Roles	***Service Owner**:* Diana Fitri, A.Md.
	***Process Owner**:* Slamet, M.T., CCNA Satria Agung Pamuji Lina Indrawati, S.Kom. Bobby Hartanto Dwi Putra Wijaya, S.Kom. Anita Izathy Chairina, S.Kom. Eva Pramita, S.Kom Rahman Nur Hadi Isnainul Amanda Perwirasari, S.Kom.
	***Process Manager**:* Sri Suhandiah, S.S., M.M Slamet, M.T., CCNA. Lina Indrawati, S.Kom
	***Process Practitioner**:* Slamet, M.T., CCNA Satria Agung Pamuji Lina Indrawati, S.Kom. Bobby Hartanto Dwi Putra Wijaya, S.Kom. Anita Izathy Chairina, S.Kom. Eva Pramita, S.Kom Rahman Nur Hadi Isnainul Amanda Perwirasari, S.Kom.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Proses layanan keluhan dijalankan oleh satu fungsi yang ada di PPTI Stikom Surabaya, yaitu *service desk*. *Service owner* untuk proses ini yaitu Diana Fitri, A.Md. Pemetaan *organizational developmet* untuk proses layanan keluhan yang ada di PPTI Stikom Surabaya dapat dilihat pada Tabel 4.4

Tabel 4.4. *Organizational Development* Layanan Keluhan

Process	Layanan Keluhan
Functions	*Service Desk*
Roles	***Service Owner**:* Diana Fitri, A.Md.
	***Process Owner**:* Diana Fitri, A.Md.
	***Process Manager**:* Sri Suhandiah, S.S., M.M Slamet, M.T., CCNA. Lina Indrawati, S.Kom
	***Process Practitioner**:* Diana Fitri, A.Md.

B. RACI *Chart*

RACI adalah sebutan akronim dari *Responsible, Accountable, Consulted,* dan *Informed.* Berikut ini adalah definisi RACI berdasarkan singkatannya.

R = *Responsible,* pihak atau orang yang bertanggung jawab untuk memastikan proses atau suatu aktivitas telah berhasil dilaksanakan.

A = *Accountable,* pihak atau orang yang memiliki kewenangan untuk menyetujui atau menerima pelaksanaan aktivitas.

C = *Consulted,* pihak atau orang yang pendapatnya dibutuhkan untuk berkonsultasi dalam suatu aktivitas.

I = *Informed,* pihak atau orang yang selalu menjaga kemajuan informasi dengan menerima informasi tentang pelaksanaan proses dan kualitas.

Tujuan dari RACI *Chart* adalah untuk menjabarkan aktivitas utama dan sub aktivitas proses bisnis yang terjadi di PPTI Stikom Surabaya, dan penanggung

jawab dari aktivitas tersebut. Aktivitas utama proses bisnis di PPTI Stikom Surabaya dari hasil wawancara (lampiran 1) terbagi menjadi empat, yaitu.

1. Menyediakan Layanan Teknologi Informasi
2. Mengembangkan Sistem Informasi yang Berjalan di Stikom Surabaya
3. Menyediakan Informasi
4. Layanan Keluhan

Sedangkan untuk mendapatkan sub aktivitas proses bisnis, diperoleh data dari tugas pokok dan fungsi PPTI Stikom Surabaya yang dapat dilihat pada lampiran 2 yang disesuaikan dengan *function* dan *roles* masing-masing unit yang dapat dilihat pada Tabel 4.1, Tabel 4.2, Tabel 4.3, dan Tabel 4.4. Hasil dari pembuatan RACI *Chart* dapat dilihat pada Gambar 4.1.

Aktivitas Penanggung Jawab / Aktivitas	Penanggung Jawab										
	Diah	Slamet	Satria	Lina	Bobby	Anita	Rahman	Mita	Amanda	Web Master	Diana
Menyediakan Layanan Teknologi Informasi											
Menjaga Sistem Jaringan Komputer beserta Koneksinya	C, I	R, A	R								
Melakukan *Recovery* Sistem Jaringan komputer dan otoritas pengguna apabila terjadi serangan atau bencana.	C, I	R, A	R								
Melakukan Pemeliharaan dan *tuning database* agar memiliki performa tinggi	C, I			R, A	R						
Mengembangkan dan Memelihara situs *web* institusi beserta aplikasinya	C, I			R, A	R	R	R	R	R	R	
Menyelenggarakan,mengelola, menjaga layanan media *online* yang berbasis *website*	C, I									R, A	

Gambar 4.1. RACI *Chart*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

C. Profil PPTI

Adapun profil PPTI yang disajikan adalah meliputi visi, misi, dan tujuan PPTI Stikom Surabaya. Berikut dapat dilihat pada Tabel 4.5 adalah.

Tabel 4.5. Profil PPTI

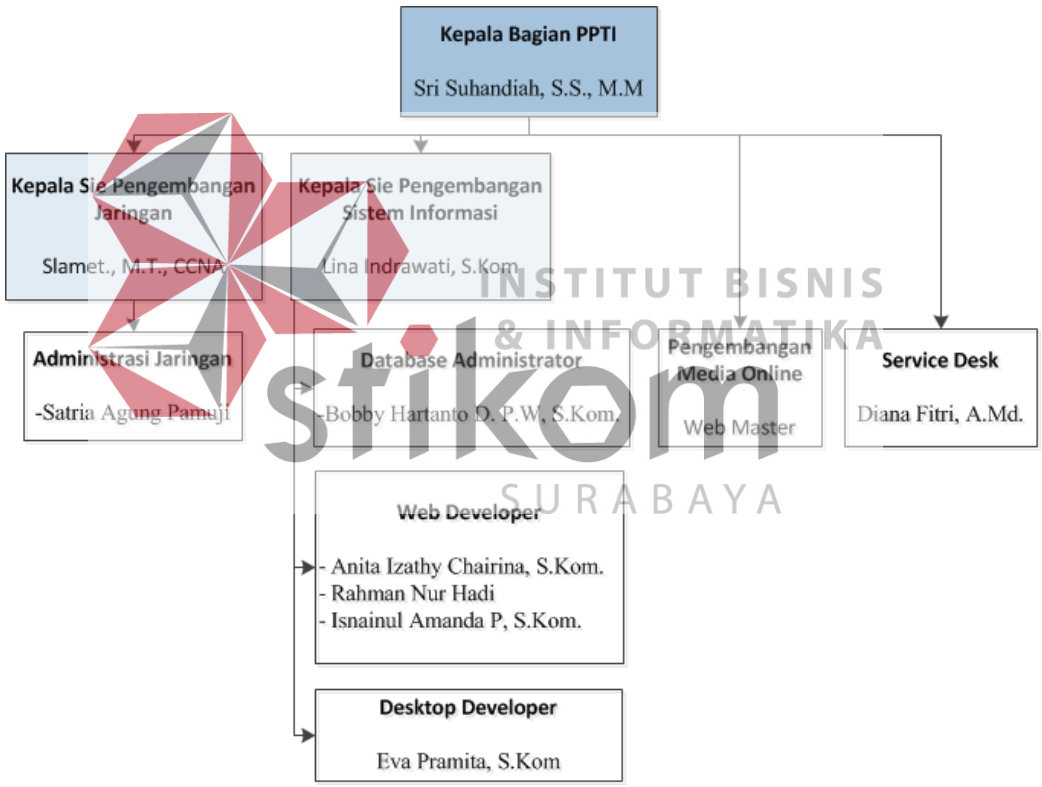
Visi
Menjadikan Institut Bisnis dan Informatika Stikom Surabaya sebagai perguruan tinggi yang unggul dan mampu bersaing di tingkat nasional melalui pengembangan dan penerapan teknologi informasi dan komunikasi.
Misi
1. Menjadikan teknologi informasi dan komunikasi sebagai sarana penunjang bagi kemajuan Institut Bisnis dan Informatika Stikom Surabaya. 2. Membangun strategi teknologi informasi dan komunikasi secara menyeluruh yang mendukung strategi Institut Bisnis dan Informatika Stikom Surabaya. 3. Melakukan inovasi dalam bidang teknologi informasi dan komunikasi sebagai upaya mengembangkan dan menyebarluaskan ilmu pengetahuan dan teknologi. 4. Menyediakan sumber daya dengan kapasitas dan kemampuan yang profesional mendukung teknologi komputasi hijau.
Tujuan
1. Menyediakan layanan berbasis teknologi informasi dan komunikasi yang terpadu untuk mendukung kegiatan akademik, administrasi, penelitian, pengabdian masyarakat dan proses belajar mengajar. 2. Menyediakan layanan teknologi informasi dan komunikasi bagi seluruh civitas akademika. 3. Menjamin tersedianya teknologi informasi dan komunikasi terkini yang dapat diandalkan serta dapat memenuhi kebutuhan pelaksanaan kegiatan.

D. Struktur Organisasi PPTI Stikom Surabaya

PPTI Stikom Surabaya dalam melakukan proses bisnis memiliki empat bagian penting dalam struktur organisasi yaitu, Bagian Pengembangan Sistem Informasi, Bagian Pengembangan Jaringan, Bagian Media *Online*, dan *Service Desk*. Keempat bagian tersebut memiliki peran yang berbeda-beda. Bagian Pengembangan Sistem Informasi dibagi menjadi dua jenis aplikasi yaitu, aplikasi *desktop* dan aplikasi *website*. Peran dari Bagian tersebut adalah melakukan

tahapan yang ada pada siklus pengembangan aplikasi pada umumnya dari tahap analisis hingga tahap uji coba dan implementasi.

Bagian Pengembangan Jaringan memiliki peran dalam melakukan pengelolaan terhadap jaringan yang sudah ada ataupun membuat jaringan baru yang berkaitan dengan jaringan *server* internet dan intranet. Bagian Media *Online* berperan dalam pengelolaan seluruh saluran *website* yang ada di Stikom Surabaya. Sedangkan *Service Desk* bertugas dalam melakukan komunikasi langsung dengan Sivitas Stikom Surabaya. Struktur organisasi dapat dilihat pada Gambar 4.2.



Gambar 4.2. Struktur Organisasi

INSTITUT BISNIS & INFORMATIKA Stikom SURABAYA

E. Kendala PPTI Stikom Surabaya

Adapun kendala-kendala yang terjadi di PPTI Stikom Surabaya adalah sebagai berikut.

1. PPTI Stikom Surabaya tidak memiliki standar keamanan informasi dan prosedur tertulis tentang kontrol keamaan.
2. PPTI Stikom Surabaya tidak memiliki prosedur baku dalam melakukan sosialisasi terhadap kebijakan keamanan informasi.
3. PPTI Stikom Surabaya tidak memiliki akses untuk memberikan informasi kepada mahasiswa ketika terjadi gangguan atau proses *maintenance* pada layanan teknologi informasi sedang dilakukan.

F. Layanan Teknologi Informasi

Layanan teknologi informasi yang telah diteliti pada peneliti sebelumnya pada tahun 2016 berjumlah 81 layanan yang terdiri dari manajerial dan operasional. Namun saat ini terdapat beberapa pengembangan layanan teknologi informasi baru yang sedang dalam proses pengerjaan. Berdasarkan 81 layanan yang ada di PPTI Stikom Surabaya, terdapat lima layanan teknologi informasi yang menjadi fokus utama karena memiliki dampak atau pengaruh besar bagi PPTI untuk terus bisa melayani kebutuhan penggunanya yaitu mahasiswa, dosen, dan karyawan. Kebutuhan tersebut berhubungan dengan aktivitas utama yang dilakukan sehari-hari di Stikom Surabaya yaitu meliputi proses akademik untuk menunjang proses belajar mengajar, sehingga layanan tersebut menjadi penting dan selalu digunakan dalam proses bisnis yang ada di Stikom Surabaya. Layanan Teknologi Informasi tersebut dapat dilihat pada Tabel 4.6.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 4.6. Layanan Teknologi Informasi PPTI Stikom Surabaya

No	Layanan TI	Deskripsi Layanan
1	Stikomapps	Merupakan layanan yang digunakan untuk mengakses kegiatan akademik seperti Sicyca dan Brilan, serta kegiatan non akademik seperti *email, drive, site*, dan lainnya.
2	Sistem Informasi *Cyber Campus* (Sicyca)	Merupakan layanan yang digunakan untuk memberikan informasi kegiatan akademik dan non-akademik kepada mahasiswa, dosen, dan karyawan. Masing-masing pengguna memiliki akses yang berbeda dalam penggunaannya. Mahasiswa memiliki akses untuk jadwal dan administrasi perkuliahan, keuangan, peminjaman buku, dan akses komunitas. Sedangkan untuk karyawan berhubungan dengan peminjaman sarana, pengecekan absensi, dan lainnya. Dosen memiliki akses yang sama dengan karyawan, namun ada fasilitas akademik untuk perkuliahan dan pengecekan data mahasiswa wali.
3	*Hybrid Learning* Stikom Surabaya (Brilian)	Merupakan layanan yang digunakan untuk proses belajar mengajar, dengan semua informasi perkuliahan seperti materi, tugas, dan ujian mata kuliah disimpan dan diakses menggunakan *Google Apps*.
4	*Wireless Connection*	Merupakan layanan yang digunakan oleh semua sivitas, baik internal maupun eksternal Stikom Surabaya untuk mengakses internet.
5	*Wired Connection*	Merupakan layanan yang digunakan oleh kalangan internal seperti dosen dan karyawan untuk mengakses internet.

INSTITUT BISNIS & INFORMATIKA Stikom SURABAYA

4.1.3 Observasi

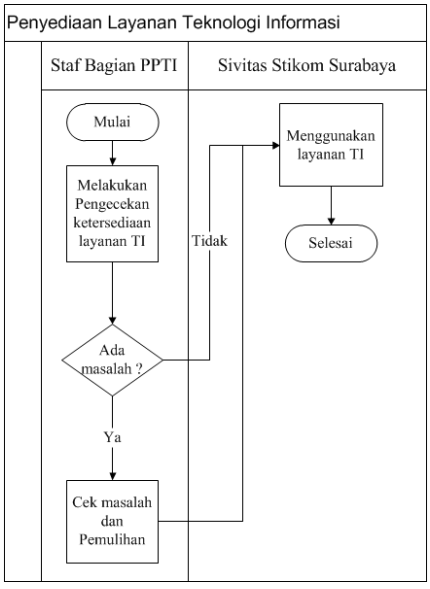
Observasi dilakukan di PPTI Stikom Surabaya, hasil dari observasi adalah berupa proses bisnis yang disajikan dalam bentuk gambar *flowchart* dan narasi. Proses bisnis yang ada di PPTI Stikom Surabaya tidak disebutkan secara rinci dalam dokumen tertulis, namun secara garis besar bisa dilihat prosesnya pada tugas pokok dan fungsi pada lampiran 2. Berikut hasil dari pelaksanaan observasi adalah.


INSTITUT BISNIS
& INFORMATIKA
stikom
SURABAYA

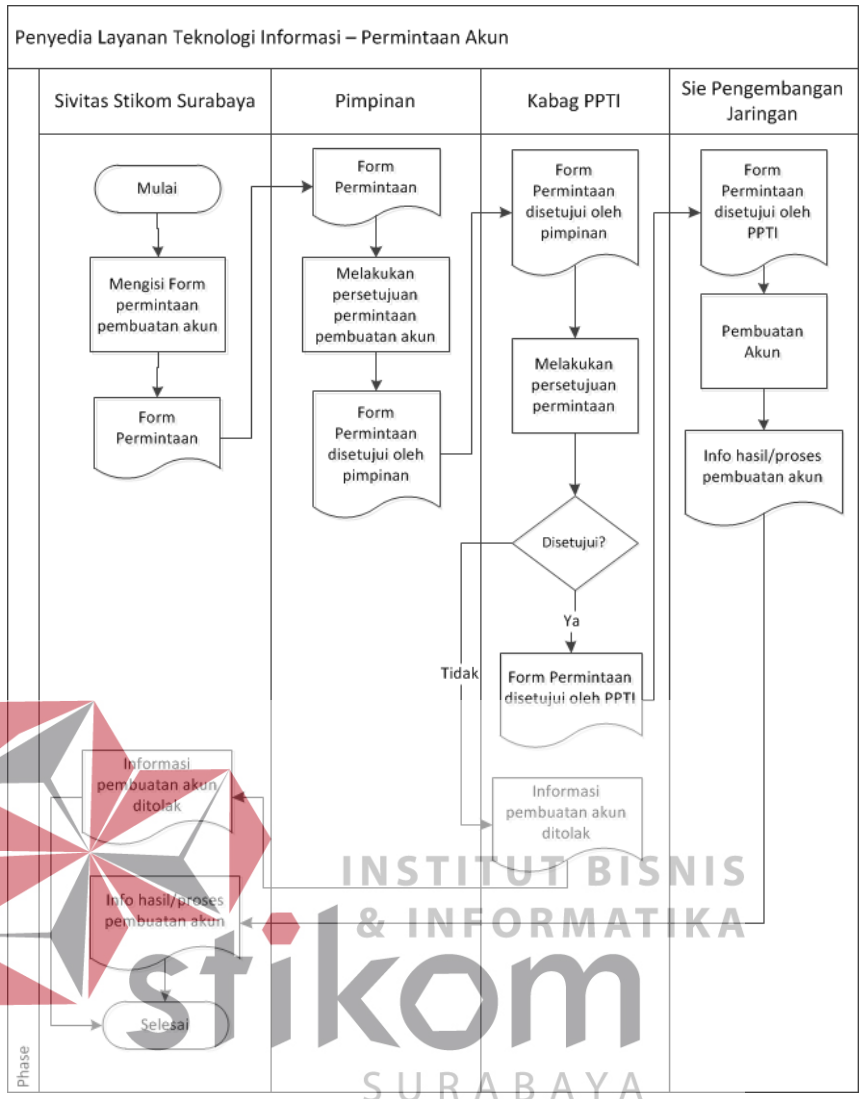
A. Proses Bisnis Penyediaan Layanan Teknologi Informasi

Proses bisnis penyediaan layanan teknologi informasi di PPTI Stikom Surabaya merupakan proses untuk menyediakan dan memantau layanan TI agar layanan TI tetap tersedia. Pada penyediaan layanan TI aktivitas yang dilakukan oleh PPTI Stikom Surabaya adalah melakukan pengecekan ketersediaan layanan TI dan melakukan aktivitas penyediaan akun (*user* dan *group*). Pengecekan ketersediaan layanan TI yang disediakan oleh PPTI termasuk Sicyca, Stikomapps, Brilian, *Wired connection*, dan *Wireless connection*. Aktor pada proses bisnis ini adalah Sivitas Stikom Surabaya dan staf bagian PPTI. Alur dimulai dari staf pengembangan bagian PPTI yang melakukan pengecekan rutin setiap harinya untuk memeriksa ketersediaan layanan TI. Jika dalam pengecekan diketahui terdapat masalah pada ketersediaan layanan TI, maka staf bagian PPTI akan melakukan proses pemulihan, sehingga sivitas Stikom Surabaya dapat menggunakan layanan TI yang disediakan oleh bagian PPTI. *Flowchart* Proses bisnis penyediaan layanan teknologi dapat dilihat pada Gambar 4.3.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA



Gambar 4.3. Proses Bisnis Penyediaan Layanan TI



Gambar 4.4. *Flowchart* Permintaan Akun

Proses penyediaan akun (*user* dan *group*) merupakan proses menyediakan akun berdasarkan permintaan dari Sivitas Stikom Surabaya. Alur ini dimulai dari sivitas yang melakukan permintaan akun dengan cara mengisi *form online* yang telah diketahui dan disetujui oleh pimpinan masing-masing. Pimpinan disini untuk bagian yaitu kepala bagian, untuk mahasiswa bisa kaprodi, dan untuk ormawa adalah koordinator ormawa. *Form online* yang telah disetujui oleh pimpinan selanjutnya diberikan ke Kabag PPTI untuk disetujui dan pengerjaan pembuatan akun dikerjakan langsung oleh sie pengembangan jaringan. Setelah pembuatan

akun selesai, maka sivitas menerima informasi bahwa akun yang telah dibuat dapat digunakan. Proses bisnis permintaan akun dapat dilihat pada Gambar 4.4.

B. Proses Bisnis Pengembangan Sistem Informasi

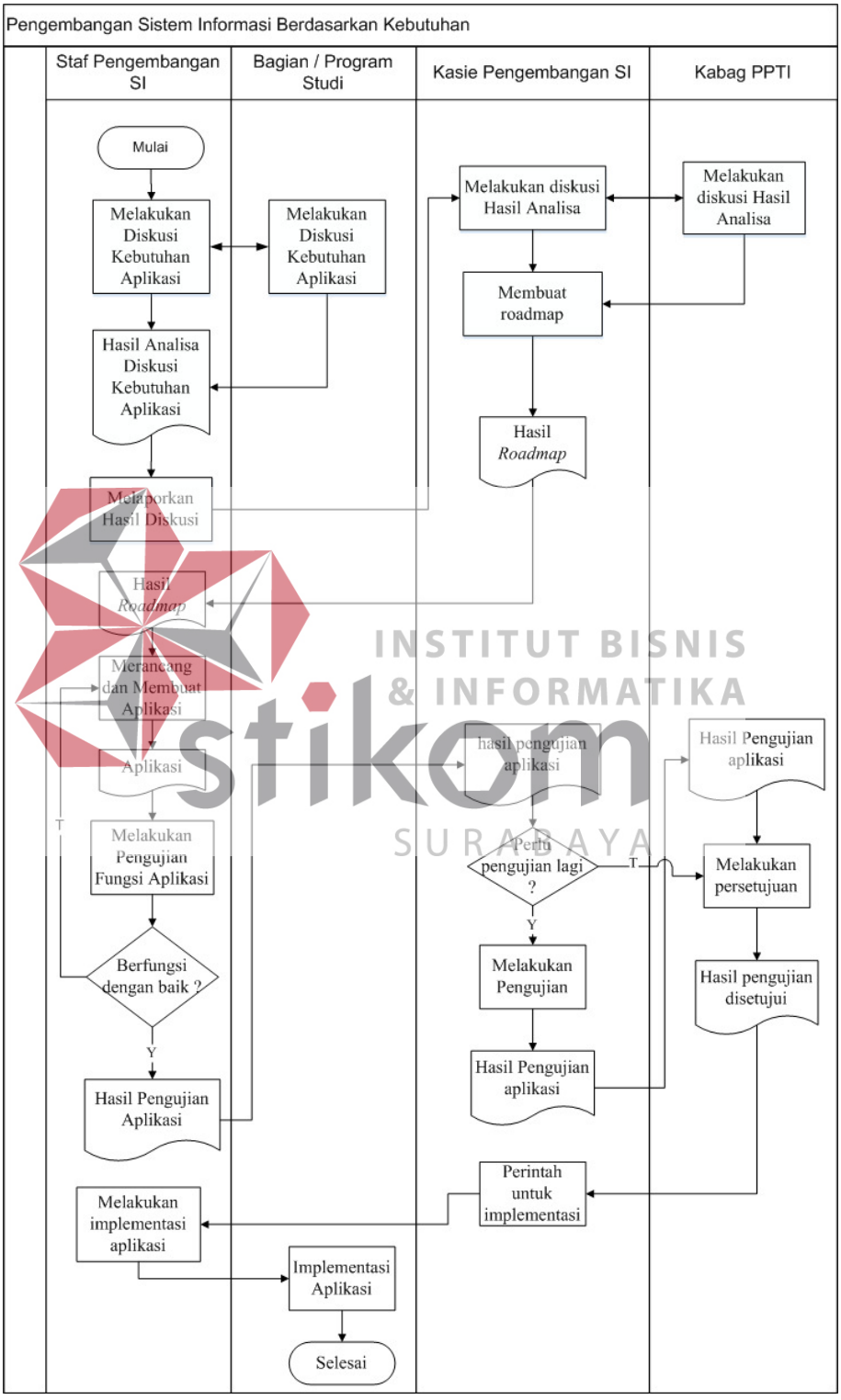
Proses bisnis pengembagan sistem informasi terbagi menjadi dua bagian, yaitu berdasarkan kebutuhan dan permintaan.

a. Kebutuhan

Pengembangan sistem informasi sesuai kebutuhan mempunyai tiga aktor yaitu staf pengembangan, kasie pengembangan SI, dan kabag PPTI. Alur proses dimulai dari staf pengembangan yang melakukan analisa kebutuhan aplikasi dengan cara mewawancarai atau melakukan diskusi dengan setiap kepala bagian atau kepala program studi untuk mengetahui kebutuhan setiap bagian. Setelah diketahui kebutuhan setiap bagian, maka staf pengembangan melaporkan dan mendiskusikan hasil analisa tersebut kepada kasie pengembangan SI dan kabag PPTI. Kabag PPTI dan kasie pengembangan SI melakukan diskusi dan membuat *roadmap* yang digunakan untuk acuan pengerjaan aplikasi. *Roadmap* diterima oleh staf pengembangan SI untuk dijadikan acuan pengerjaan aplikasi. Aplikasi yang sudah diselesaikan akan diuji oleh staf pengembangan SI dan hasil pengujian diberikan kepada kasie pengembangan SI. Kasie pengembangan SI akan melakukan pemeriksaan apakah aplikasi perlu diuji kembali. Jika perlu diuji kembali maka kasie pengembangan SI melakukan pengujian dan memberikan hasil pengujian kepada Kabag PPTI. Hasil pengujian aplikasi yang ditunjukkan kepada Kabag PPTI disetujui dan aplikasi yang sudah berfungsi dengan baik akan diimplementasikan dan dapat digunakan oleh Bagian/Program Studi.

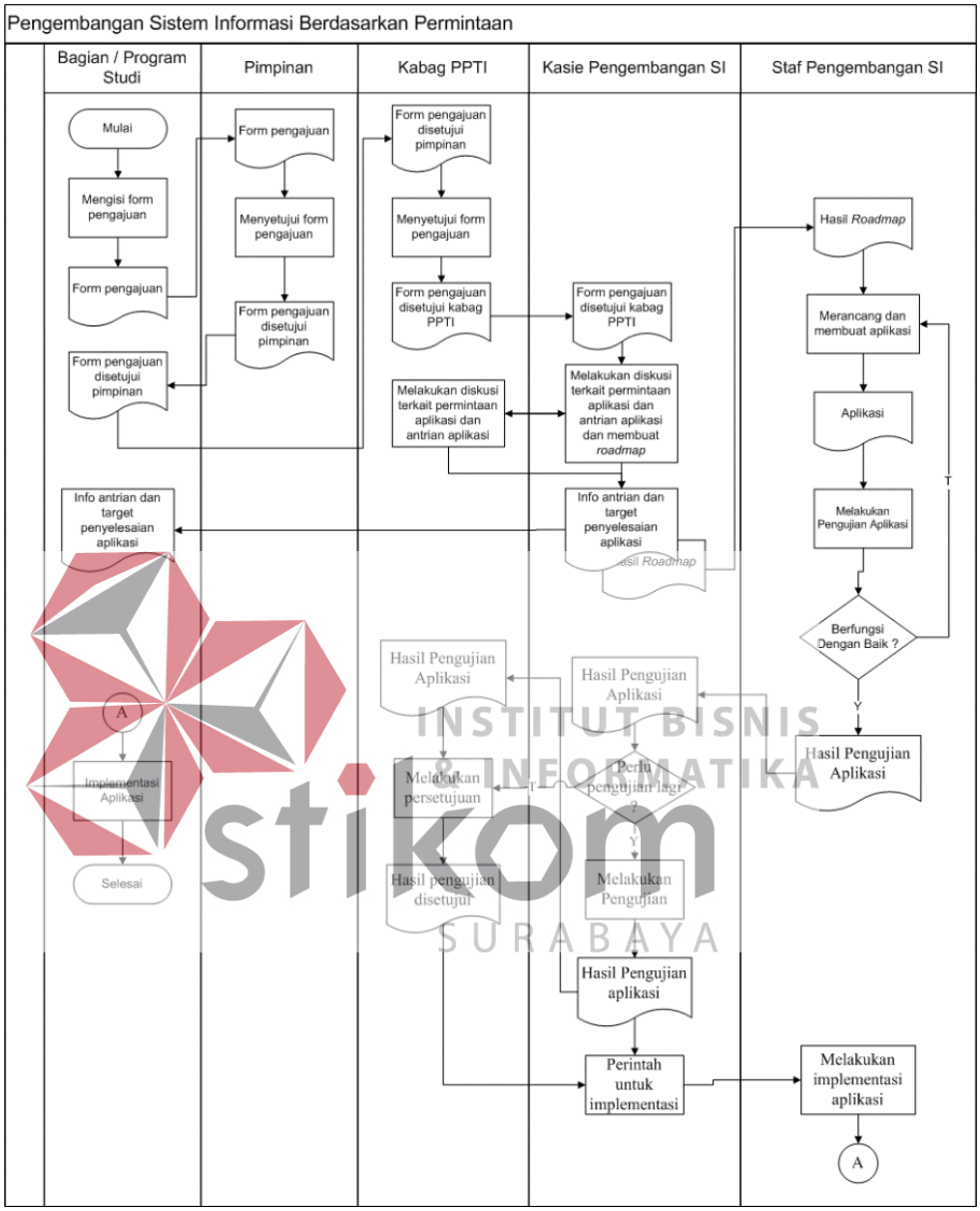
INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Flowchart proses bisnis pengembangan sistem informasi berdasarkan kebutuhan dapat dilihat pada Gambar 4.5.



Gambar 4.5. Proses Bisnis Pengembangan SI Kebutuhan

b. Permintaan



Gambar 4.6. Proses Bisnis Pengembangan SI Permintaan

Pengembangan sistem informasi sesuai permintaan mempunyai empat aktor yaitu bagian Stikom Surabaya, staf pengembangan, kasie pengembangan sistem informasi, dan kabag PPTI. Alur dimulai dari bagian yang mengajukan permintaan pengembangan sistem informasi (SI) melalui *form online*, *form*

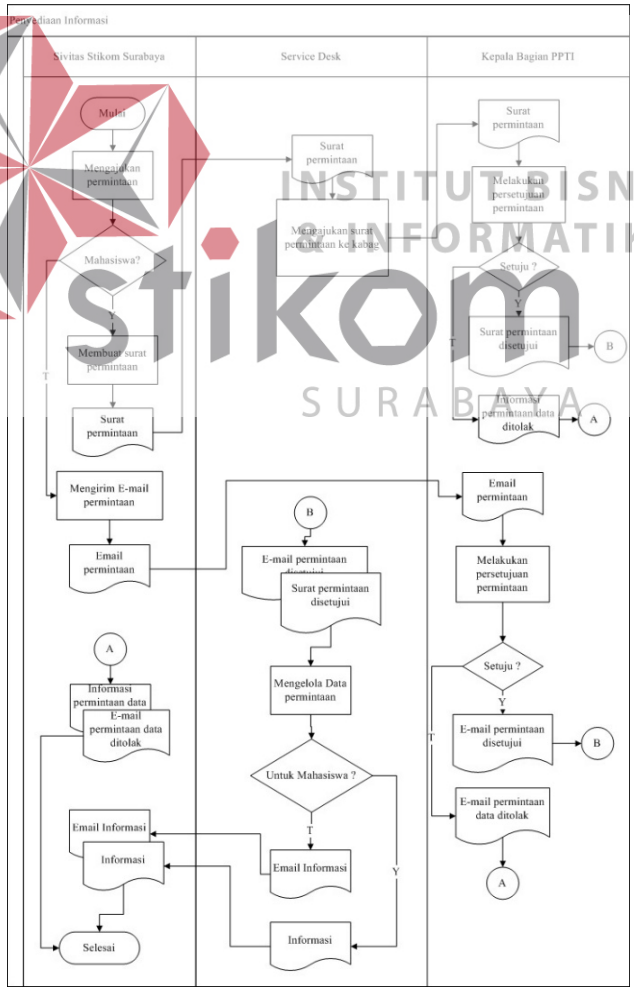
online tersebut telah diketahui oleh pimpinan atau atasan yang membawahi suatu bagian/program studi. Form pengajuan pengembangan SI diterima oleh kabag PPTI untuk disetujui. Setelah form pengajuan disetujui, kabag PPTI Stikom Surabaya dan kasie pengembangan SI melakukan diskusi terkait target penyelesaian, nomor antrian dan pembuatan *roadmap*. Selanjutnya, antrian dan target waktu penyelesaian diinfokan langsung kepada bagian dan *roadmap* diterima oleh staf pengembangan untuk segera melakukan pengembangan aplikasi. Aplikasi yang sudah diselesaikan akan diuji oleh staf pengembangan SI dan hasil pengujian diberikan kepada kasie pengembangan SI. Kasie pengembangan SI akan melakukan pemeriksaan apakah aplikasi perlu diuji kembali. Jika perlu diuji kembali maka kasie pengembangan SI melakukan pengujian dan memberikan hasil pengujian kepada Kabag PPTI. Hasil pengujian aplikasi yang ditunjukkan kepada Kabag PPTI disetujui dan aplikasi yang sudah berfungsi dengan baik akan diimplementasikan dan dapat digunakan oleh Bagian/Program Studi. *Flowchart* proses bisnis pengembangan sistem informasi berdasarkan permintaan dapat dilihat pada Gambar 4.6.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

C. Proses Bisnis Penyediaan Informasi

Proses bisnis penyediaan informasi adalah proses untuk menyediakan informasi berdasarkan permintaan dari sivitas Stikom Surabaya. Aktor pada proses ini yaitu sivitas Stikom Surabaya, *service desk*, dan kabag PPTI. Alur dimulai dari adanya permintaan data oleh sivitas Stikom Surabaya. Jika mahasiswa, maka dimulai dengan menyerahkan surat permintaan ke *service desk* yang ditujukan untuk kabag, sedangkan untuk dosen atau karyawan dapat melalui *email* yang ditujukan kepada kabag PPTI. *Service desk* memberikan surat

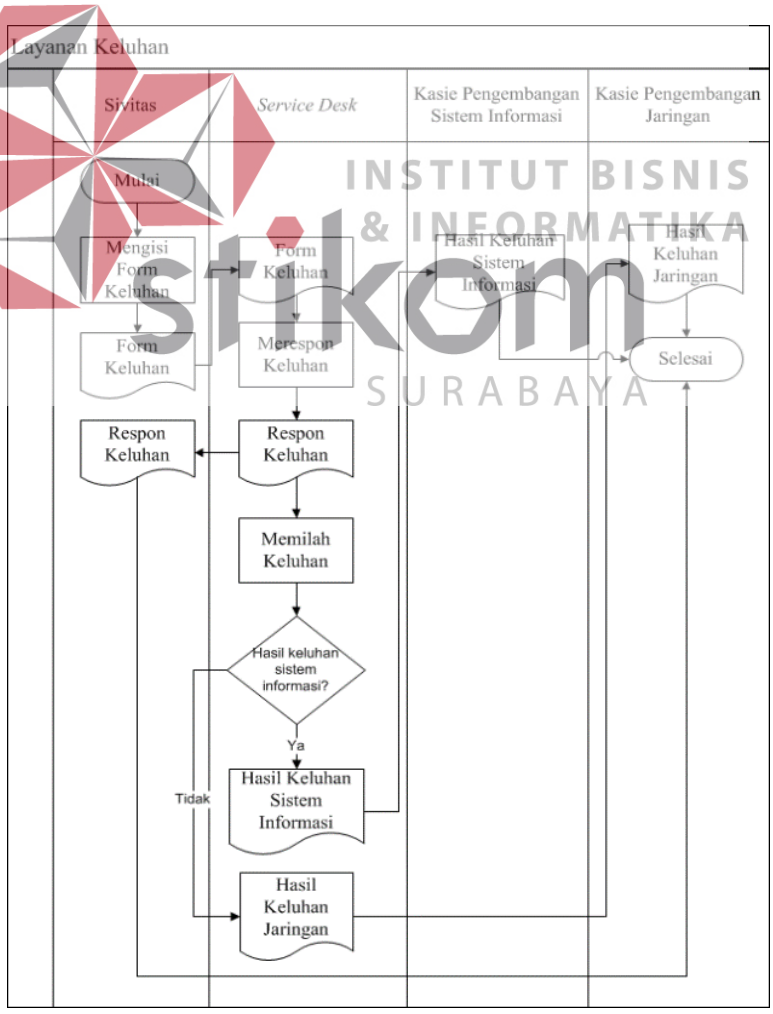
pengajuan dari mahasiswa kepada kabag PPTI untuk disetujui. *Email* dan surat permintaan diperiksa oleh Kabag PPTI untuk disetujui. Jika Surat dan email permintaan disetujui, maka surat dan email permintaan akan diteruskan kepada *service desk* untuk dilakukan pengolahan data. Jika surat dan *email* permintaan tidak disetujui, maka sivitas menerima informasi jika surat/email permintaan ditolak. Selanjutnya informasi yang sudah dibuat oleh *service desk* untuk mahasiswa akan diberikan kepada mahasiswa berupa *hard copy* sedangkan informasi untuk karyawan akan dikirimkan melalui email. *Flowchart* proses bisnis penyediaan informasi dapat dilihat pada Gambar 4.7.



Gambar 4.7. Proses Bisnis Penyediaan Informasi

D. Proses Bisnis Layanan Keluhan

Aktor pada proses ini adalah Sivitas Stikom Surabaya, *service desk*, kasie pemgembangan SI dan kasie pengembangan jaringan. Proses bisnis dimulai dari *service desk* menerima keluhan dari pelanggan, kemudian *ervice desk* memberikan respon kepada Sivitas bahwa bagian PPTI segera memeriksa gangguan dan melaporkan hal tersebut ke kasie terkait untuk ditangani. Setelah itu, *service desk* memilah keluhan tersebut sesuai dengan jenis keluhan (sistem informasi dan jaringan). *Flowchart* proses bisnis penanganan keluhan dapat dilihat pada Gambar 4.8.



Gambar 4.8. Proses Bisnis Layanan Keluhan

4.2 Tahap Pengembangan

Pada tahap pengembangan menghasilkan sembilan dokumen yang terdiri dari, sebagai berikut.

1. Dokumen kebijakan keamanan informasi.
2. Dokumen klasifikasi aset.
3. Dokumen penilaian risiko.
4. Dokumen insiden keamanan layanan teknologi informasi.
5. Dokumen tinjauan keamanan.
6. Dokumen SOP sosialisasi kebijakan keamanan informasi, dokumen ini meliputi standar sosialisasi kebijakan keamanan informasi, prosedur sosialisasi kebijakan keamanan informasi, dan formulir sosialisasi kebijakan keamanan informasi yang meliputi formulir rancangan sosialisasi, formulir daftar sosialisasi, dan formulir laporan hasil sosialisasi.
7. Dokumen SOP klasifikasi aset, dokumen ini meliputi standar klasifikasi aset, prosedur klasifikasi aset, dan formulir klasifikasi aset.
8. Dokumen SOP kontrol keamanan, dokumen ini meliputi standar kontrol keamanan, prosedur kontrol keamanan, dan formulir kontrol keamanan yang meliputi formulir tindakan ancaman dan formulir analisis temuan.
9. Dokumen SOP pengelolaan insiden keamanan teknologi informasi, dokumen ini meliputi standar pengelolaan insiden keamanan teknologi informasi, prosedur pengelolaan insiden keamanan teknologi informasi, dan formulir insiden, formulir penyelesaian insiden, dan formulir rekapitulasi insiden.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Dokumen SOP yang dihasilkan dari pembuatan *information security management* hanya digunakan oleh internal PPTI Stikom Surabaya, sehingga dokumen tersebut bersifat rahasia dan tidak dapat dipublikasikan.

4.2.1 Membuat dan Merevisi *Information Security Policy*

Pada tahap ini menghasilkan dokumen kebijakan keamanan informasi. Adapun kebijakan keamanan informasi tersebut memuat tentang penggunaan dan penyalahgunaan aset TI, kontrol akses, kontrol *password*, pengendalian *email*, anti-virus, klasifikasi informasi, klasifikasi dokumen, akses jarak jauh, pelanggaran hak cipta, pembuangan aset, dan retensi *record.*

Pada tahap membuat dan merevisi kebijakan keamanan informasi ini dapat dijelaskan dalam *mapping* yang bertujuan untuk pemberian solusi dengan melihat dari sisi ITIL versi 3 dan PPTI Stikom Surabaya.

Tabel 4.7. *Mapping* Kebijakan

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
Membuat dan Merevisi *Information Security Policy*	Di dalam ITIL telah dijelaskan bahwa Kegiatan pengelolaan keamanan informasi harus difokuskan dan didorong oleh kebijakan keamanan informasi yang meliputi kebijakan: 1. Kebijakan Keamanan Informasi Secara Umum 2. Kebijakan penggunaan dan penyalahgunaan aset TI. 3. Kebijakan Kontrol Akses	Secara tertulis PPTI Stikom Surabaya saat ini dalam hal keamanan informasi hanya memiliki Kebijakan Internet yang digunakan dalam pengelolaan layanan *Wired Connection* dan *Wireless Connection.*	Solusi yang diberikan adalah membuat kebijakan-kebijakan yang ada di ITIL dengan cara digabung menjadi satu dokumen yaitu dokumen kebijakan keamanan informasi.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 4.7 (Lanjutan)

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
	4. Kebijakan Kontrol *Password* 5. Kebijakan Email 6. Kebijakan Internet 7. Kebijakan Anti-Virus 8. Kebijakan Klasifikasi Informasi 9. Kebijakan Klasifikasi Dokumen 10. Kebijakan Akses Jarak Jauh 11. Kebijakan Pemasok 12. Kebijakan Pelanggaran Hak Cipta 13. Kebijakan Penyusutan Aset, dan 14. Kebijakan Retensi *Record*		

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Setiap dokumen kebijakan memiliki enam poin yang dijadikan format penyusunan kebijakan yang dapat dilihat pada Tabel 4.8.

Tabel 4.8. Penjelasan Format Kebijakan

Poin	Deskripsi
1. Objektif	Objektif menjelaskan keadaan yang ingin dicapai dengan pembuatan tersebut.
2. Tujuan Kebijakan	Tujuan menjelaskan hal yang ingin dicapai dengan dibuatnya kebijakan tersebut.
3. Ruang Lingkup	Ruang lingkup yang dimaksud yaitu proses bisnis apa saja yang akan terlibat dalam kebijakan tersebut.
4. Deskripsi	Deskripsi menjelaskan apa yang menjadi batasan dan aturan dalam kebijakan tersebut.
5. Komitmen	Komitmen menjelaskan perjanjian yang harus dipenuhi oleh pihak yang dituju dalam

Tabel 4.8 (Lanjutan)

Poin	Deskripsi
	menerapakan kebijakan tersebut.
6. Larangan dan Sanksi	Larangan dan sanksi menjelaskan apa yang terjadi jika aturan dilanggar atau perjanjian yang dijelaskan di dalam komitmen tidak sesuai dengan yang dilakukan.

Dokumen kebijakan keamanan informasi memuat informasi tentang objektif dan tujuan dari pembuatan kebijakan, ruang lingkup kebijakan, deskripsi kebijakan, komitmen yang harus dipenuhi, dan larangan serta sanksi yang diterima apabila melanggar kebijakan. Dokumen Kebijakan keamanan informasi dapat dilihat pada Tabel 4.9.

Tabel 4.9. Kebijakan Keamanan Informasi

1. Objektif	Keamanan Informasi
2. Tujuan Kebijakan	Pengembangan dan Penerapan Teknologi Informasi (PPTI) Stikom Surabaya memiliki kebijakan untuk mengelola keamanan informasi.
3. Ruang Lingkup	Memuat kebijakan keamanan informasi yang meliputi penggunaan dan penyalahgunaan aset teknologi informasi (TI), kontrol akses, kontrol *password*, *email*, anti-virus, klasifikasi informasi, klasifikasi dokumen, akses jarak jauh, pelanggaran hak cipta untuk elektronik, pembuangan aset, dan retensi *record.*
4. Deskripsi	1. Pengguna adalah seluruh Mahasiswa, Dosen, dan Staf Institut Bisnis dan Informatika Stikom Surabaya 2. Pengelola adalah bagian Pengembangan dan Penerapan Teknologi Informasi Stikom Surabaya (PPTI). 3. *Virtual Private* merupakan suatu koneksi antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan Internet. 4. Aset yang dikelola PPTI Stikom Surabaya adalah aset teknologi informasi berupa data, informasi, atau dokumen, perangkat lunak, dan perangkat keras. 5. Penggunaan dan Penyalahgunaan aset TI merupakan kegiatan yang menggambarkan penggunaan terhadap suatu aset layanan teknologi informasi, dan penyalahgunaan atau penggunaan aset layanan teknologi informasi secara illegal yang mengakibatkan kerugian atau kerusakan.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

	6. Kontrol akses merupakan kegiatan pembatasan akses secara umum dengan selektif untuk kegiatan

Tabel 4.9. (Lanjutan)

4. Deskripsi	memasuki dan menggunakan tempat atau suatu sumber daya. 7. Kontrol *password* merupakan kegiatan pembatasan akses yang didadasarkan dengan menggunakan karakter khusus. 8. *Email* merupakan pesan yang didistribusikan dengan sarana elektronik dari satu pengguna komputer ke satu atau lebih penerima melalui jaringan. 9. Anti-virus merupakan perangkat lunak yang dirancang untuk mencegah, mendeteksi, dan menghapus virus dari komputer. Klasifikasi informasi merupakan kategorisasi materi informasi sensitif yang memerlukan perlindungan kerahasiaan, integritas, dan ketersediaan dan dilindungi pada tingkat yang sesuai. 10. Klasifikasi dokumen merupakan kategorisasi dokumen ke dalam satu atau lebih dari tingkat jenis dokumen yang sesuai. 11. Akses jarak jauh merupakan kegiatan yang mengacu pada kemampuan untuk mengakses sumber daya atau komputer dari lokasi yang jauh. 12. Pelanggaran hak cipta untuk elektronik merupakan suatu kegiatan untuk mengatur penyalahgunaan terhadap hak cipta. 13. Penyusutan aset merupakan kegiatan pengelolaan dengan cara pelepasan aset, seperti penjualan, pembongkaran, relokasi, pemusnahan. 14. Retensi *record* merupakan kegiatan membuat penentuan jangka waktu simpan berdasarkan nilai guna.
5. Komitmen	Adapun komitmen yang harus dipenuhi dari kebijakan keamanan informasi adalah meliputi keamanan informasi secara umum, penggunaan dan penyalahgunaan aset teknologi informasi (TI), kontrol akses, kontrol *password*, *email*, anti-virus, klasifikasi informasi, klasifikasi dokumen, akses jarak jauh, pelanggaran hak cipta untuk elektronik, penyusutan aset, dan retensi *record.* Keamanan Informasi Secara Umum: 1. PPTI Stikom Surabaya bertanggung jawab untuk melakukan sosialisasi kebijakan keamanan informasi. 2. PPTI Stikom Surabaya harus memastikan pengguna menaati ketentuan yang telah

INSTITUT BISNIS & INFORMATIKA Stikom SURABAYA

	ditetapkan oleh Institut Bisnis dan Informatika Stikom Surabaya.

Tabel 4.9. (Lanjutan)

5. Komitmen	3. PPTI Stikom Surabaya memastikan pengguna menerima sanksi apabila melanggar ketentuan yang telah ditetapkan. 4. PPTI Stikom Surabaya melakukan kontrol keamanan dengan cara menerapkan jenis kontrol keamanan dan harus ditinjau secara berkala, minimal setiap tahun. Penggunaan dan Penyalahgunaan aset TI: 1. Setiap aktivitas penggunaan aset yang dimiliki harus didukung dengan proses pendokumentasian. 2. Setiap aset yang dikembangkan harus dilakukan pemantauan dengan melakukan kategori atau klasifikasi aset. 3. PPTI Stikom Surabaya harus menjaga dan melindungi aset yang dimiliki. 4. PPTI Stikom Surabaya bertanggung jawab dalam melakukan pengelolaan terhadap insiden yang dilaporkan pengguna terkait layanan teknologi informasi. 5. PPTI Stikom Surabaya bertanggung jawab memberikan pelayanan terhadap penggunaan teknologi informasi, baik berhubungan dengan penyediaan maupun peningkatan layanan. 6. Apabila ada pemindahan aset yang ditujukan kepada pihak ketiga (misalnya untuk *maintenance*), maka seksi yang bertanggung jawab harus memastikan sudah tidak ada data rahasia di dalamnya. Kontrol Akses: 1. Setiap aplikasi, dan manajemen jaringan yang ada di PPTI Stikom Surabaya harus memiliki *role* hak akses baik ke dalam aplikasi atau *database* yang harus disetujui oleh kepala seksi pengembangan jaringan atau seksi pengembangan sistem informasi, dan ditinjau secara berkala. 2. Setiap instalasi *router*, aplikasi, atau *tools*, dan akses ke jaringan harus memiliki ijin dari kepala seksi yang bertanggung jawab langsung terhadap aktivitas tersebut. 3. *Password* merupakan suatu bentuk dari data orientasi rahasia yang digunakan untuk

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 4.9. (Lanjutan)

5. Komitmen	mengontrol akses ke dalam suatu sumber informasi. Kontrol *Password*: 1. PPTI Stikom Surabaya memberikan *password* kepada pengguna untuk mengakses sistem maupun aplikasi. 2. PPTI Stikom Surabaya harus membuat manajemen *password* dengan menentukan panjang *password* dan kriteria *password* yang kuat dan aman. PPTI Stikom Surabaya memastikan pengguna bertanggung jawab terhadap kerahasiaan *password* yang dimiliki. 3. PPTI Stikom Surabaya memberikan arahan kepada pengguna untuk mengganti *password* secara berkala, minimal 3 bulan sekali. 4. PPTI Stikom Surabaya memastikan penggunaan *password* adalah merupakan hal yang sensitif, sehingga penyimpanan *password* harus menggunakan teknik enkripsi atau bentuk yang tidak mudah untuk dibaca, dan penggunaan teknik tersebut harus ditinjau secara berkala sesuai dengan perkembangan teknologi. *Email*: 1. PPTI Stikom Surabaya memberikan alamat *email* kepada pengguna dengan akhiran @stikom.edu untuk dipergunakan sebagaimana mestinya. 2. PPTI Stikom Surabaya bertanggung jawab dalam melakukan perlindungan ataupun pengelolaan *email* pengguna yang telah terdaftar. 3. *Email* Organisasi tidak boleh digunakan untuk kepentingan dan tujuan komersial pribadi. 4. *Email* tidak boleh digunakan untuk kegiatan melanggar hukum. Anti-Virus: 1. Setiap aset yang dimiliki harus memiliki proteksi untuk menghindari gangguan keamanan informasi. 2. Untuk melakukan proteksi dan atau pencegahan terhadap gangguan keamanan seperti *malware* atau virus pada aset informasi, PPTI Stikom

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

	Surabaya menggunakan antivirus, *firewall,* enkripsi, dan penggunaan *patch* yang tepat, dan akan diperbaharui secara berkala.

Tabel 4.9. (Lanjutan)

5. Komitmen	Klasifikasi Informasi: 1. Informasi diklasifikasi untuk kebutuhan, prioritas, dan tingkat perlindungannya. 2. Klasifikasi Informasi dapat dikategorikan menjadi 4, yaitu: a. *Confidential*, informasi yang bersifat rahasia dan hanya diketahui oleh orang yang berkepentingan (*top level management*) dan mempunyai hak resmi terhadap informasi tersebut. b. *Restricted*, informasi yang terbatas atau sensitif yang digunakan untuk penggunaan atau tujuan resmi, seperti keuangan dan kontrak kerja (*medium level management).* c. *Internal Use Only*, informasi data pribadi atau milik perseorangan yang bukan merupakan informasi untuk umum. d. *Public*, informasi yang dapat diakses oleh semua orang secara bebas. Klasifikasi Dokumen: 1. Akses terhadap dokumen dan proses bisnis harus dikontrol dengan dasar kebutuhan bisnis dan keamanan. 2. Klasifikasi dokumen dapat dikategorikan menjadi 4, yaitu: a. *Public*, informasi di dalam dokumen yang tersedia untuk umum dan ditujukan untuk distribusi di luar organisasi tanpa adanya risiko bahaya, seperti majalah organisasi dan brosur lowongan pekerjaan. b. *Confidential*, informasi di dalam dokumen yang bersifat rahasia dan hanya diketahui oleh orang yang berkepentingan, seperti dokumen identitas pribadi karyawan dan laporan akuntansi atau gaji. c. *Internal Use Only*, informasi di dalam dokumen yang tidak disetujui untuk dipublikasikan di luar organisasi, dan dokumen hanya digunakan untuk kepentingan organisasi, seperti dokumen rapat dan laporan proyek internal. d. *Secret*, informasi di dalam dokumen yang sangat sensitif atau sangat rahasia, seperti

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

	dokumen strategi investasi dan dokumen

Tabel 4.9. (Lanjutan)

5. Komitmen	rencana atau desain produk atau layanan baru. Akses Jarak Jauh: 1. Akses jarak jauh harus dikontrol dengan menggunakan enkripsi yaitu *Virtual Private.* 2. Saat menggunakan komputer yang memiliki jarak jauh untuk terhubung ke jaringan perusahaan, Pengguna resmi harus memastikan *host* jarak jauh tidak terhubung ke jaringan lain pada saat bersamaan. Pelanggaran Hak Cipta: 1. PPTI Stikom Surabaya memastikan apabila pengguna melakukan penggandaan aset baik sebagian atau keseluruhan harus melalui ijin. 2. PPTI Stikom Surabaya menindaklanjuti pengguna yang melakukan pelanggaran hak cipta secara tegas dengan pencabutan hak akses terhadap aset secara sementara ataupun secara tetap. Penyusutan Aset: 1. Penyusutan aset dilakukan jika aset tidak dapat digunakan lagi secara permanen berhenti beroperasi dan tidak memiliki nilai kegunaan di masa yang akan datang. Penyusutan aset dilakukan dengan cara penjualan, pembongkaran, relokasi, dan pemusnahan. 2. Transaksi penghapusan aset harus dikomunikasikan dan dikoordinasikan dengan kepala bagian, kepala seksi jaringan, dan kepala seksi sistem informasi, serta harus sepengetahuan pihak luar yang berhubungan langsung dengan aset yang dikelola PPTI Stikom Surabaya seperti Bagian Administrasi Umum, dan disetujui oleh wakil rektor terkait. 3. Semua transaksi penghapusan aset harus dicatat dan ditinjau oleh seksi pengembangan jaringan, seksi pengembangan sistem informasi dan kepala bagian PPTI Stikom Surabaya. Retensi *Record:* 1. PPTI Stikom Surabaya membuat jadwal retensi

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

	aset yang menjelaskan jangka waktu suatu aset harus disimpan sesuai dengan nilai kegunaan.

Tabel 4.9. (Lanjutan)

5. Komitmen	2. Transaksi retensi aset harus dikomunikasikan dan dikoordinasikan dengan kepala bagian, kepala seksi jaringan, dan kepala seksi sistem informasi. 3. Semua transaksi retensi aset harus dicatat dan ditinjau oleh seksi pengembangan jaringan, seksi pengembangan sistem informasi dan kepala bagian PPTI Stikom Surabaya.
6. Larangan dan Sanksi	Larangan yang tidak boleh dilakukan oleh pengguna, yaitu: 1. Pengguna dilarang melakukan segala macam usaha/tindakan yang mengarah pada penggunaan manipulasi yang merugikan pengguna lainnya serta bertentangan dengan kebijakan keamanan informasi di Institut Bisnis dan Informatika Stikom Surabaya. 2. Pengguna dilarang melakukan penggandaan aset baik sebagian atau keseluruhan dan sabotase terhadap aset informasi atau hal lain yang berkaitan dengan pelanggaran hak cipta, tanpa seijin pihak pengelola. Jika ada pelanggaran yang dilakukan, sanksi yang diterima oleh pengguna yaitu: 1. Pencabutan hak akses terhadap layanan yang digunakan sementara, dilakukan dengan surat teguran atau peringatan secara tertulis melalui email kepada pengguna. 2. Pencabutan hak akses layanan tetap, penghentian dilakukan jika terjadi penggunaan diluar batas toleransi yang diberikan sesuai dengan aturan yang telah ditetapkan dalam Peraturan Kepegawaian Tahun 2014 dan Keputusan Rektor Nomor 266/KPT-03C/VII/2015 tentang Penegakan Norma Pendidikan bagi Mahasiswa

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

4.2.2 Mengkomunikasikan Semua Kebijakan Keamanan Informasi

Pada tahap mengkomunikasikan semua kebijakan keamanan informasi ini dapat dijelaskan dalam *mapping* yang bertujuan untuk pemberian solusi dengan melihat dari sisi ITIL versi 3 dan PPTI Stikom Surabaya.

Tabel 4.10. *Mapping* Sosialisasi Kebijakan

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
Mengkomunikasikan Semua Kebijakan Keamanan Informasi	Di dalam ITIL dijelaskan pada proses manajemen keamanan informasi harus disertakan proses produksi, pemeliharaan, pendistribusian, dan penegakan kebijakan keamanan informasi.	PPTI Stikom Surabaya tidak memiliki Standar tertulis tentang cara mengkomunikasikan kebijakan-kebijakan yang telah dimiliki.	Solusi yang diberikan adalah membuat SOP Sosialisasi Kebijakan Keamanan Informasi yang diturunkan dari kebijakan keamanan informasi pada bagian komitmen poin nomor 1 tentang keamanan informasi secara umum. Tujuan SOP ini adalah untuk memberikan pemahaman kepada pengguna dan menjamin kontiunitas bisnis dengan memberikan pelayanan informasi kepada pengguna sesuai dengan kebutuhan.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Keluaran dari tahap ini adalah dokumen SOP sosialisasi kebijakan keamanan informasi yang terdiri dari standar sosialisasi kebijakan keamanan informasi, prosedur sosialisasi kebijakan keamanan informasi, dan tiga formulir yang meliputi formulir rancangan sosialisasi, formulir daftar sosialisasi, dan formulir laporan hasil sosialisasi. Standar sosialisasi kebijakan keamanan informasi dapat dilihat pada Tabel 4.11.

Tabel 4.11. Standar Sosialisasi Kebijakan Keamanan Informasi

1. Visi dan Misi Organisasi	Visi dan Misi Organisasi
2. Rasionale	Alasan pembuatan standar sosialisasi kebijakan keamanan informasi
3. Pihak yang bertanggung jawab untuk memenuhi isi standar	Pihak yang berwenang bedasarkan tugas dan tanggung jawab masing-masing staf

Tabel 4.11. (Lanjutan)

4. Definisi Istilah	Menjelaskan definisi semua istilah yang digunakan dalam standar.
5. Pernyataan Isi Standar	Isi standar secara umum
6. Strategi	Strategi dalam menjalankan standar sosialisasi kebijakan keamanan informasi.
7. Indikator	Ukuran keberhasilan dari proses sosialisasi kebijakan keamanan informasi
8. Dokumen Terkait	Dokumen yang terkait dengan dokumen sosialisasi kebijakan keamanan informasi
9. Referensi	Referensi yang digunakan dalam membuat standar.

Isi Standar menjelaskan tentang visi misi kampus, *rasionale* atau tujuan dari standar, pihak yang bertanggung jawab untuk memenuhi isi standar, definisi istilah untuk kata-kata asing atau istilah, pernyataan isi standar, strategi yang mendukung isi standar, indikator, dokumen terkait, dan referensi yang digunakan untuk menyusun standar. Prosedur Sosialisasi Kebijakan Keamanan Informasi dapat dilihat pada Tabel 4.12.

Tabel 4.12. Prosedur Sosialisasi Kebijakan Keamanan Informasi

1. Tujuan Prosedur	Menjelaskan tujuan dalam pelaksanaan proses sosialisasi kebijakan keamanan informasi..
2. Luas Lingkup SOP dan Penggunaannya	Menjelaskan ruang lingkup prosedur yang dirancang.
3. Standar	Menjelaskan standar yang digunakan sebagai acuan dalam pembuatan prosedur.
4. Definisi Istilah	Istilah-istilah yang ada sudah dituliskan pada Definisi Istilah yang terdapat di dokumen Standar Sosialisasi Kebijakan Keamanan Informasi.
5. Prosedur	1. PPTI Stikom Surabaya melakukan perencanaan untuk melakukan sosialisasi. (*Plan).*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

	2. PPTI Stikom Surabaya melakukan implementasi sosialisasi sesuai perencenaan. (*Do*) 3. PPTI Stikom Surabaya mencatat hasil implementasi ke dalam dokumen sosialisasi. (*Do)* 4. PPTI Stikom Surabaya melakukan evaluasi berdasarkan dokumen sosialisasi. (*Check)* 5. PPTI Stikom Surabaya melakukan tindakan perbaikan atau pengembangan sesuai hasil evaluasi untuk kedepannya. (*Action*).

Tabel 4.12. (Lanjutan)

6. Kualifikasi Pejabat/Petugas yang menjalankan SOP	Petugas yang berwenang dalam pelaksanaan proses berdasarkan tugas dan tanggung jawab masing-masing staf.
7. Bagan Alir Prosedur	Menggambarkan alur proses melakukan sosialisasi kebijakan keamanan informasi.
8. Catatan	Berisikan catatan yang diperlukan dalam menjalankan prosedur.
9. Referensi	Referensi yang digunakan dalam membuat prosedur.

Isi prosedur menjelaskan tentang tujuan prosedur, luas dan lingkup SOP, standar yang dituju, defenisi istilah asing dalam prosedur yang dibuat, isi atau penjelasan dari prosedur, petugas yang menjalankan prosedur, bagan atau alir prosedur, catatan terkait prosedur, dan referensi yang digunakan dalam pembuatan prosedur.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

4.2.3 Mengakategorikan Aset-Aset Informasi

Pada tahap mengkategorikan aset-aset informasi ini dapat dijelaskan dalam *mapping* yang bertujuan untuk pemberian solusi dengan melihat dari sisi ITIL versi 3 dan PPTI Stikom Surabaya.

Tabel 4.13. *Mapping* Kategori Aset Informasi

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
Mengkategorikasi aset-aset informasi	Di dalam ITIL dijelaskan dalam kunci aktivitas manajemen keamanan informasi salah	Di PPTI Stikom Surabaya tidak ada sumber tertulis tentang klasifikasi aset-aset informasi.	Solusi yang diberikan adalah membuat dokumen klasifikasi aset dengan

Tabel 4.13. (Lanjutan)

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
	satunya adalah melakukan klasifikasi semua aset dan melakukan dokumentasi terhadap aset-aset tersebut.	Namun pada penelitian yang sebelumnya di PPTI Stikom Surabaya telah dibuatkan klasifikasi tersebut yang dimuat dalam dokumen *Service Portofolio.* Namun, masih ada beberapa informasi yang tidak lengkap atau poin yang belum diisi.	melakukan pembaharuan atau *update* terhadap dokumen *service portfolio* dan membuat SOP Klasifikasi Aset yang diturunkan dari kebijakan keamanan informasi pada bagian komitmen poin nomor 2 tentang penggunaan dan penyalahgunaan aset TI.

Berikut ini adalah keluaran dari tahap mengkategorikan aset-aset informasi adalah sebagai berikut.

A. Dokumen Klasifikasi Aset

Tujuan dari dokumen ini adalah untuk dokumentasi tertulis tentang layanan, sebagai bahan evaluasi bagi PPTI Stikom Surabaya dalam melakukan pengembangan layanan TI. Pembuatan dokumen klasifikasi aset ini melakukan pembaharuan dari penelitian terdahulu tentang *service portfolio.* Pada dokumen *service portfolio* memuat informasi berupa nama layanan, status layanan, jenis layanan, pemilik layanan, pelanggan, kontak, prosedur, layanan yang diberikan, infrastruktur layanan, komponen, dan rencana pengembangan. Dokumen *service portfolio* dapat dilihat pada Gambar 4.9.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

LAYANAN SISTEM INFORMASI / APLIKASI	
Layanan	SICYCA
Status Siklus Hidup Layanan	Layanan yang Digunakan
Jenis Layanan	Layanan Sistem Informasi yang memberikan informasi tentang kegiatan akademik dan non akademik.
Pemilik Layanan	PPTI Stikom Surabaya
Pelanggan	Mahasiswa Stikom Surabaya Dosen Stikom Surabaya Karyawan Stikom Surabaya
Kontak	Hotline PPTI: 089647313348 (WA/Telp/SMS) 08123287190 (WA/Telp/SMS)
Prosedur	Mendatangi pihak PPTI dan meminta layanan yang di inginkan.
Layanan yang Diberikan	
Infrastruktur Layanan	1. Jaringan internet 2. Server 3. *Unit Power Supplay* (UPS) 4. Listrik 5. Pegawai atau karyawan
Komponen	1. SIIS Lama. 2. Dashboard. 3. Menu Akademik. 4. Menu Keuangan. 5. Menu Perpustakaan. 6. E - Resource. 7. Menu PPTA. 8. Menu Komunitas. 9. Feedback.
Perubahan yang direncanakan	-

Gambar 4.9. Dokumen *Service Portfolio*

Pembaharuan yang dilakukan adalah mengklasifikasikan aset dari sisi komponen *tools* dan sisi fungsi layanan bagi kebutuhan pengguna dengan menambahan deskripsi komponen aset dan pengembangan infrsatruktur dari sisi *tools* yang digunakan aset.

Dokumen klasifikasi aset yang dibuat terdiri dari lima klasifikasi layanan yaitu *Sicyca, Stikomapps, Brilian, Wired Connection,* dan *Wireless Connection.* Sebagai contoh dalam pembuatannya dapat dilihat pada Tabel 4.14 dan 4.15 yang membahas tentang klasifikasi Stikomapps. Dokumen klasifikasi aset lainnya dapat dilihat pada buku *output* dari tugas akhir ini.

Tabel 4.14. Klasifikasi Aset Sisi Komponen *Tools*

Nama Aset	Stikomapps
Jenis Aset	Layanan Sistem Informasi tentang akademik dan non-akademik
Pemilik Aset	PPTI Stikom Surabaya
Deskripsi Aset	Merupakan layanan yang digunakan untuk mengakses kegiatan akademik seperti Sicyca dan Brilan, serta kegiatan non akademik seperti *email*, *drive*, *site*, *calendar*, dan *google+*.
Kelebihan dan Kelemahan Aset	Kelebihan: Menggunakan *single sign on* yang bisa digunakan untuk mengakses aplikasi akademik.
	Kelemahan: Tidak bisa akses brilian dan aplikasi lainnya jika tidak melalui Stikomapps.
Rencana Pengembangan	-

***Tools* Stikomapss**

No	*Tools*	Kegunaan *Tools*
1	Internet Service Provider Telkom	Koneksi jaringan
2	Server Amazon Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz Memory 4Gb Hdd 7.8 Gb	Komputer *Server*
3	Ubuntu 14.04.5 LTS	Sistem Operasi
4	MySQL	*Database*
5	Oracle Database 11G	*Database*
6	Apache2	*Web Server*
7	SSH	*Remote Server*
8	Chkrootkit	*Cek Hack*
9	SNMP	*Agen Monitoring*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Tabel 4.15. Klasifikasi Aset Sisi Fungsi Kebutuhan Pengguna

Klasifikasi Aset Pengguna Stikomapps Berdasarkan Mahasiswa		
Pengguna		Mahasiswa
Deskripsi Kebutuhan Pengguna		Mahasiswa membutuhkan layanan TI yang dapat memberikan informasi seputar kegiatan akademik dan kampus. Dalam menunjang kegiatan pembelajaran, mahasiswa juga membutuhkan layanan TI edukasi untuk memudahkan kegiatan proses belajar yang langsung mengarah pada matakuliah yang bersangkutan.
Fungsi Pada Layanan Stikomapss		
No	**Fungsi**	**Deskripsi Fungsi**
1	Agenda	Konten yang digunakan untuk membagikan pengumuman dan agenda agenda stikom Surabaya.
2	Email	Aplikasi *electronic mail* yang digunakan dalam bertukar data ataupun informasi.
3	Kalender	Aplikasi yang digunakan untuk memudahkan pengguna dalam membuat jadwal atau agenda.
4	Drive	Aplikasi yang digunakan untuk menyimpan *file*, membuat dan menyunting dokumen, dan mengakses fitur google lainnya.
5	Site	Aplikasi yang digunakan untuk membuat situs *web*.
6	Google+	Aplikasi media sosial yang dimiliki Google.
7	*Link* ke Aplikasi Akademik	Aplikasi akademik beberapa diantaranya adalah Sistem informasi *cyber campus* (Sicyca), pusat pelayanan tugas akhir (ppta), *digital library*, *electronic resources* Stikom Surabaya, dan aplikasi saran dan keluhan.
8	*Link* ke Unit Kegiatan Mahasiswa	Unit kegiatan mahasiswa yang meliputi tari, musik, g-forst, silat tauhid Indonesia, jiujitsu, Capoeira, Stikom *English community*, pasukan pengibar bendera, korps sukarela, himpunan pecinta alam, futsal, dan bulu tangkis
9	Link ke Unit Kegiatan Kerohanian	Unit kegiatan kerohanian yang meliputi Kristen protestan, budha, islam, hindu dan katolik.
10	Stikom *Links*	Stikom *links* yang meliputi *website* stikom Surabaya dan *website* prodi-prodi yang ada di Stikom Surabaya.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Pada klasifikasi aset dari sisi komponen *tools* memuat informasi berupa nama layanan, jenis layanan, pemilik layanan, deskripsi layanan, kelebihan dan kelemahan layanan, rencana pengembangan, dan *tools* yang menjadi pengembangan aset. Sedangkan klasifikasi aset dari sisi fungsi layanan pada kebutuhan pengguna memuat informasi berupa pengguna, deskripsi kebutuhan pengguna, dan fungsi apa saja yang ada pada suatu layanan berserta deskripsinya.

B. SOP Klasifikasi Aset

Dokumen SOP klasifikasi aset merupakan dokumen yang bertujuan untuk menjelaskan cara mengklasifikasikan aset dari sisi komponen *tools* dan sisi fungsi layanan bagi kebutuhan pengguna, dokumen ini meliputi standar klasifikasi aset, prosedur klasifikasi aset, dan formulir klasifikasi aset. Dokumen SOP klasifikasi aset dapat dilihat pada dokumen *output information security management.*

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

4.2.4 Menilai, Meninjau, dan Melaporkan Risiko Keamanan dan Ancaman

Pada tahap menilai, meninjau, dan melaporkan risiko keamanan dan ancaman dapat dijelaskan dalam *mapping* yang bertujuan untuk pemberian solusi dengan melihat dari sisi ITIL versi 3 dan PPTI Stikom Surabaya.

Tabel 4.16. *Mapping* Penilaian Risiko

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
Identifikasi risiko dan ancaman keamanan	Di ITIL dalam proses manajemen keamanan informasi diperlukan adanya pengelolaan risiko yang terkait dengan akses terhadap layanan, informasi dan	PPTI Stikom Surabaya tidak memiliki laporan tertulis tentang adanya risiko dan ancaman.	Solusi yang diberikan adalah membuat dokumen penilaian risiko yang bertujuan untuk mengidentifikasi dan menilai risiko ataupun ancaman terhadap keamanan informasi.

Tabel 4.16. (Lanjutan)

Proses	ITIL Versi 3	PPTI Stikom Surabaya	Solusi
	sistem.		
Penilaian Risiko	Di dalam ITIL telah dijelaskan salah satu *output* dari ISM adalah membuat atau melakukan revisi terhadap proses penilaian risiko keamanan yang telah ada.	PPTI Stikom Surabaya belum memiliki standar untuk menilai suatu risiko. Namun, pada penelitian sebelumnya yang mengambil topik di PPTI telah membuat dokumen penilaian risiko yang tercantum dalam proses *availability management.*	Solusi yang diberikan adalah melakukan pembaharuan terhadap dokumen penilaian risiko pada dokumen *availability management.* Format penilaian risiko yang digunakan mengikuti ISO 27001.

Keluaran dari proses ini adalah dokumen penilaian risiko, berikut ini adalah penjelasan dari dokumen penilaian risiko.

A. Dokumen Penilaian Risiko

Tujuan dari dibuatkannya dokumen penilaian risiko adalah untuk mengetahui ancaman-ancaman dari luar yang berpotensi mengganggu keamanan informasi organisasi dan potensial kelemahan yang mungkin dimiliki oleh informasi di organisasi.

Dokumen penilaian risiko dari tugas akhir ini dibuat dengan melakukan revisi dari dokumen penilaian risiko penelitian terdahulu dalam proses *availability management*, adapun alasan untuk melakukan revisi adalah karena proses yang dilakukan dalam penilaian risiko tersebut tidak dijelaskan secara rinci tentang daftar risiko apa yang timbul dari setiap aset, dan proses penilaian risiko yang dilakukan juga tidak menggunakan perhitungan rumus yang jelas. Dokumen

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

availability management pada proses penilaian risiko dapat dilihat pada Gambar 4.10.

Risk Analysis

Kejadian	Penyebab	Dampak	Mitigasi	Unit yang Bertanggung Jawab
Stikomapps down	1.Listrik Padam 2.Kerusakan server (*hard disk bad sector*)	Seluruh pengguna (dosen, karyawan, mahasiswa) tidak bisa akses	1. Memastikan suhu komputer *server* tetap dingin dan bersih dari debu-debu yang menempel 2. Penggunakan PSU berkualitas untuk menjaga arus-arus yang tidak diinginkan dari PLN	*Staff* pengembangan Sistem Informasi

Risk Assesment

Nama layanan	Tingkat kerusakan (%) dalam 1 tahun	*Unit responsible*
SICYCA	<1	Pengembangan Jaringan dan Pengembangan Sistem Informasi

Gambar 4.10. Penilaian Risiko Pada *Availability Management*

Berdasarkan dokumen tersebut, dilakukan pembaharuan dokumen penilaian risiko. Berikut ini adalah langkah-langkah dan hasil yang diperoleh dalam melakukan penilaian terhadap suatu risiko.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

1. Identifikasi Aset

Langkah yang pertama adalah melakukan identifikasi aset, Identifikasi dilakukan untuk mengelompokkan aset ke dalam beberapa kategori atau golongan, agar lebih mudah dalam melakukan tahapan penilaian risiko. Pada tahap Identifikasi menjelaskan nama aset dan jenis aset. Nama aset untuk lima layanan PPTI Stikom Surabaya, dan jenis aset yang terdiri dari pengembangan sistem informasi dan pengembangan jaringan. Identifikasi aset dapat dilihat pada Tabel 4.17.

Tabel 4.17. Identifikasi Aset

No	Nama Aset	Jenis Aset
1	Sicyca	Pengembangan Sistem Informasi
2	Stikomapps	Pengembangan Sistem Informasi
3	Brilian	Pengembangan Sistem Informasi
4	*Wired Connection*	Pengembangan Jaringan
5	*Wireless Connection*	Pengembangan Jaringan

2. Menghitung Nilai Aset

Menghitung nilai aset adalah menghitung nilai informasi yang dimiliki oleh organisasi. Cara menghitung nilai aset dapat berdasarkan aspek keamanan inforrmasi yaitu, kerahasiaan (*Confidentiality),* keutuhan *(Integrity),* dan ketersediaan (*Availability).* Menghitung nilai aset dapat dilihat pada Tabel 4.18.

Tabel 4.18. Nilai Aset

Nama Aset	Kriteria			Nilai Aset (NC+NI+NV)
	Nilai Confidentiality (NC)	Nilai Integrity (NI)	Nilai Availability (NV)	
Sicyca	4	3	4	11
Stikomapps	4	3	4	11
Brilian	2	2	4	8
Wired Connection	2	3	4	9
Wireless Connection	2	3	4	9

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

3. Mengidentifikasi Ancaman dan Kelemahan yang dimiliki oleh aset

Tujuan dari mengindentifikasi ancaman dan kelemahan adalah agar diketahui ancaman yang mungkin terjadi dan membahayakan sistem dalam organisasi dan memahami kelemahan yang dimiliki dalam mengelola suatu aset informasi.

4. Menentukan Kemungkinan (*Probability*)

Tujuan dari tahapan ini adalah untuk mengetahui kemungkinan ancaman yang timbul sesuai dengan identifikasi ancaman dan kelemahan. Metode untuk menentukan probabilitasn atau kemungkinan (*Probability*) berdasarkan historis kejadian ancaman sebelumnya, atau ditentukan berdasarkan pengamatan kondisi yang dapat dinilai. Identifikasi ancaman, kelemahan, dan probabilitas dapat dilihat pada Tabel 4.19.

a. Identifikasi Ancaman dan Kelemahan Sicyca

Tabel 4.19. Identifikasi Ancaman dan Kelemahan Sicyca

Nama Aset	Sicyca		
Jenis Aset	Sistem Informasi		
Risiko	**Jenis Kejadian**	**Probabilitas**	**Rata-rata Probabilitas**
Bencana Alam dan politik	*Threat*	*Low*	0.1
Power Failure	*Threat*	*Low*	0.3
Software Failure	*Threat*	*Medium*	0.5
Hardware Failure	*Threat*	*Low*	0.1
Application Failure/Error (include Logic)	*Vulnerable*	*Medium*	0.5
Network Failure	*Vulnerable*	*Medium*	0.4
Virus Attack (Trojan, Worm, dll)	*Threat*	*Low*	0.1
Data Corruption	*Vulnerable*	*Medium*	0.1
Human error	*Vulnerable*	*Low*	0.3
Akses Ilegal	*Threat*	*High*	0.1
Jumlah Ancaman = 10	**Jumlah rata-rata probabilitas**		**2.5**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah Ancaman 2.5 / 10 = 0.25**		

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Identifikasi pada aset Sicyca memiliki 10 ancaman, dengan jumlah rata-rata probabilitasnya 2.5, dan nilai ancamannya adalah 0.25. Identifikasi ancaman, kelemahan, dan probabilitas pada Stikomapps dapat dilihat pada Tabel 4.20.

b. Identifikasi Ancaman dan Kelemahan Stikomapps

Tabel 4.20. Identifikasi Ancaman dan Kelemahan Stikomapps

Nama Aset	Stikomapps		
Jenis Aset	Sistem Informasi		
Risiko	**Jenis Kejadian**	**Probabilitas**	**Rata-rata Probabilitas**
Bencana Alam dan politik	*Threat*	*Low*	0.1
Power Failure	*Threat*	*Low*	0.1
Software Failure	*Threat*	*Medium*	0.5
Hardware Failure	*Threat*	*Low*	0.1
Application Failure/Error(include Logic)	*Vulnerable*	*Medium*	0.5
Network Failure	*Vulnerable*	*Low*	0.4
Virus Attack (Trojan, Worm, dll)	*Threat*	*Low*	0.1
Data Corruption	*Vulnerable*	*Medium*	0.1
Human error	*Vulnerable*	*Low*	0.3
Akses Ilegal	*Threat*	*High*	0.1
Jumlah Ancaman = 10	**Jumlah rata-rata probabilitas**		**2.3**
Nilai Threat (NT)	**Jumlah rata-rata probabilitas / Jumlah Ancaman 2.3 / 10 = 0.23**		

Identifikasi pada aset Stikomapps memiliki 10 ancaman, dengan jumlah rata-rata probabilitasnya 2.3, dan nilai ancamannya adalah 0.23. Identifikasi ancaman, kelemahan, dan probabilitas pada Brilian dapat dilihat pada Tabel 4.21.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

No	Ruang Lingkup	Pertanyaan	Jawaban
3.	Proses Bisnis Perusahaan	Apa saja proses bisnis yang ada di PPTI Stikom Surabaya saat ini?	1. Penyediaan layanan teknologi informasi (pengecekan kinerja jaringan dan internet, permintaan akun dan blog) 2. Pengembangan sistem informasi dalam Stikom Surabaya (pengembangan sistem informasi berdasarkan permintaan dan pengembangan sistem informasi berdasarkan kebutuhan) 3. Penyediaan informasi 4. Layanan keluhan
4.	Fitur baru pada lima prioritas layanan TI	Apakah ada fitur baru pada lima prioritas layanan dan jika ada, apa saja fitur yang ditambahkan?	1. Pada Brilian, fitur plagiarism diganti dari turnitin ke plagscan 2. Pada Sicyca, untuk dosen dan karyawan terdapat fitur peminjaman internet, permintaan akun (Blog dosen dan *web* prodi), akses khusus wifi, laporan dosen wali (absensi, nilai, dan tunggakan) dan fitur peminjaman ruang perpus. 3. Pada Sicyca, untuk mahasiswa terdapat fitur tambahan untuk pengajuan blog organisasi dan akun (admin dan domain)
5.	Alasan lima prioritas layanan TI	Mengapa Sicyca, Stikomapps, Brilian, *Wired*, dan *Wireless* menjadi layanan prioritas pada PPTI ?	Kelima layanan mendukung proses akademik pada Stikom Surabaya dan mempunyai dampak yang besar bagi Stikom Surabaya.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

No	Ruang Lingkup	Pertanyaan	Jawaban
6.	Penanggung jawab layanan TI	Siapa saja penangggung jawab untuk masing-masing layanan?	1. Sicyca : Sie Pengembangan Sistem Informasi 2. Stikomapps : Sie Pengembangan Sistem Informasi 3. Brilian : Sie Pengembangan Sistem Informasi 4. *Wired Connection :* Sie Pengembangan Jaringan 5. *Wireless Connection :* Sie Pengembangan Jaringan
7.	*Information security policy*	Apakah PPTI Stikom Surabaya memiliki kebijakan tertulis tentang *information security* ?	Belum memiliki kebijakan *information security*, hanya memiliki kebijakan internet.
8	Standar, Prosedur, Formulir sosialisasi kebijakan keamanan informasi	Apakah PPTI Stikom Surabaya memiliki Standar, prosedur, formulir sosialisasi kebijakan keamanan informasi?	Belum memiliki standar, prosedur, formulir sosialisasi kebijakan keamanan informasi.
9	Standar, Prosedur, Formulir pengelolaan insiden keamanan teknologi informasi	Apakah PPTI Stikom Surabaya memiliki Standar, prosedur, formulir pengelolaan insiden keamanan teknologi informasi?	Sudah memiliki standar, prosedur, dan formulir pengelolaan insiden. Namun, masih terlalu kompleks dan rumit. Membutuhkan banyak sekali pencatatan untuk menangani satu insiden, sehingga menghabiskan banyak waktu.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

No	Ruang Lingkup	Pertanyaan	Jawaban
10	Standar, Prosedur, Formulir kontrol keamanan	Apakah PPTI Stikom Surabaya memiliki Standar, prosedur, formulir kontrol keamanan?	Belum memiliki standar, prosedur, formulir kontrol keamanan.
11.	Alur sosialisasi kebijakan keamanan informasi	Bagaimana alur sosialisasi kebijakan?	1. Biasanya untuk karyawan dan dosen disampaikan melalui bagian personalia. 2. Untuk mahasiswa disampaikan melalui bagian kemahasiswaan. 3. Dan juga dilakukan publikasi melalui media *online* dan media cetak. 4. Biasanya juga dilakukan pelatihan secara terbuka bagi Sivitas Stikom Surabaya.
12	Alur pengelolaan insiden	Bagaimana alur pengelolaan insiden?	1. Adanya keluhan atau insiden diterima dari *service desk.* 2. *Service desk* melakukan respon terhadap adanya keluhan tersebut tentang sedang diperbaiki/sedang dicek. 3. *Service desk* meneruskan informasi keluhan kepada kasie yang berwenang. 4. Kasie dan staf yang bertanggung jawab atas pemulihan insiden/keluhan tersebut melakukan perbaikan layanan. 5. Apabila keluhan telah diselesaikan/belum bisa diselesaikan, *service desk* tetap memberikan informasi kepada pelapor. 6. Alur pelaporan insiden biasanya menggunakan telepon, email, dan melalui

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

No	Ruang Lingkup	Pertanyaan	Jawaban
			aplikasi.
13	Akses kepada Sivitas Stikom Surabaya	Apakah PPTI Stikom Surabaya memiliki akses untuk memberitahu Sivitas perihal layanan TI yang sedang dalam keadaan tidak stabil/sedang dalam keadaan *maintenance?*	Tidak memiliki akses untuk memberi tahu kepada mahasiswa untuk layanan yang sedang dalam perbaikan atau *maintenance.* Jika pemberitahuan untuk dosen bisa melalui email, dan untuk kedepannya *website* PPTI akan ada pemberitahuan semacam itu.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

Lampiran 2**.** Tugas Pokok dan Fungsi PPTI

Bagian Pengembangan dan Penerapan Teknologi Informasi (PPTI) adalah unsur unit pelaksana teknis di bidang pengembangan dan penerapan teknologi informasi yang berfungsi menjamin berlangsungnya semua kegiatan operasional yang memanfaatkan perangkat teknologi informasi serta melakukan penerapan teknologi baru untuk meningkatkan efisiensi pekerjaan. PPTI dipimpin oleh Kepala Bagian (Kabag) yang bertanggung jawab kepada Wakil Rektor Bidang Akademik. PPTI membawahi seksi-seksi, yaitu Seksi Pengembangan Jaringan, Seksi Pengembangan Aplikasi, dan Seksi Media *Online.*

Tugas Pokok Kabag PPTI:

Kabag PPTI memiliki tugas pokok sebagai berikut:

1. Mengoordinasikan penyusunan *blue print* pengembangan Bagian PPTI dan *road map* pencapaiannya sesuai dengan Rencana Strategi (Renstra) STIKOM Surabaya yang meliputi model pengelolaan dan pengembangan teknologi informasi dan sumber daya manusia (SDM).
2. Menyusun rencana proker beserta anggaran kerja tahunan PPTI sebagai pedoman kerja berdasarkan *blue print* dan *road map* PPTI.
3. Melaksanakan proker dan mengendalikan anggaran kerja tahunan PPTI.
4. Mengevaluasi pelaksanaan proker dan anggaran PPTI sebagai bahan pertimbangan dalam penyusunan rencana proker dan anggaran di tahun berikutnya.
5. Merancang dan mengoordinasi pembuatan aplikasi untuk kebutuhan operasional internal.
6. Melakukan pemeliharaan perangkat keras jaringan, aplikasi internal, dan data untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi, antara

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

lain: melakukan proses *back up*, menentukan kontrol hak akses, melakukan dokumentasi aplikasi internal, kontrol manajemen jaringan, dan lain-lain.

7. Melakukan pengontrolan secara menyeluruh terhadap keamanan meliputi keamanan fisik, keamanan personel, keamanan operasi, keamanan komunikasi, kemanan jaringan, dan keamanan informasi.
8. Melakukan otentifikasi dan otorisasi pengguna maupun pihak ketiga.
9. Menjalankan fungsi data-center (dokumen digital dan data) untuk mengakomodasi seluruh kebutuhan Stikom Surabaya.
10. Memberikan pelayanan *help-desk* berkaitan dengan fasilitas aplikasi internal dan jaringan STIKOMNet.
11. Melakukan evaluasi dan menjaga keberlangsungan pengembangan dan penerapan teknologi informasi.
12. Memberikan masukan bagi kebutuhan sistem dan teknologi informasi bagi unit kerja lain yang membutuhkan.

Wewenang Kabag PPTI

Kabag PPTI memiliki wewenang sebagai berikut.

1. Atas seijin pimpinan institusi, melakukan perubahan atau penyesuaian *blue print* ataupun *road map* pengembangan sistem dan teknologi informasi.
2. Atas seijin pimpinan institusi, melakukan perubahan atau penyesuaian proker dan anggaran tahun PPTI.
3. Memberi peringatan dan/atau membatalkan aplikasi internal yang dibuat tanpa persetujuan PPTI.
4. Melakukan interupsi terhadap komunikasi jaringan Stikom Surabaya untuk tujuan pemeliharaan sistem.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

5. Melakukan interupsi terhadap usaha-usaha yang mengancam keamanan personel, operasi, komunikasi, jaringan, dan informasi.
6. Memberikan bantuan konsultasi tentang perancangan aplikasi untuk kebutuhan operasional internal.
7. Memberikan usulan dan masukan kepada atasan langsung dalam hal pengembangan bagian PPTI.

Tugas Pokok Seksi Pengembangan Jaringan

Kasi Pengembangan Jaringan memiliki tugas pokok sebagai berikut.

1. Mendesain dan mengimplementasikan sistem jaringan komputer dan yang akan digunakan organisasi.
2. Menjaga kinerja sistem jaringan komputer beserta koneksinya.
3. Menjaga keamanan sistem jaringan komputer bebas dari gangguan serangan dan ancaman internal maupun eksternal.
4. Melakukan *recovery* sistem jaringan komputer dan otoritas pengguna apabila terjadi serangan atau bencana.
5. Mengelola *user* dan *group* yang ada yaitu otentifikasi, otorisasi pengguna sampai kode etik penggunaan *resources.*
6. Menerapkan sistem *back up resources* untuk menjaga ketersediaan data dan informasi apabila dibutuhkan.
7. Melakukan dokumentasi prosedur penanganan sistem jaringan komputer.
8. Membantu manajemen pemilihan teknologi agar tersedia sistem jaringan komputer yang skalabel sebagaimana diterapkan organisasi.
9. Memberikan bantuan bagi pengguna yang mengalami gangguan atas sistem jaringan komputer.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

10. Membantu bagian perencanaan untuk menyediakan prosedur kerja dalam memanfaatkan sistem komputer dan jaringan yang sesederhana mungkin bagi pengguna.

Tugas Pokok Seksi Pengembangan Aplikasi

Kasi Pengembangan Aplikasi memiliki tugas pokok sebagai berikut.

1. Menyusun rencana pengembangan sistem informasi yang terintegrasi.
2. Mengkoordinasikan sistem informasi yang dikembangkan di unit kerja menuju sistem informasi yang terintegrasi.
3. Membantu menentukan dan / atau mengembangkan sistem informasi atau aplikasi pada bagian lain yang membutuhkan.
4. Melaksanakan sosialisasi dan/atau pelatihan pemanfaatan aplikasi baru kepada para pengguna seluruh institusi dengan atau tanpa bekerja sama dengan unit kerja lain.
5. Membantu melayani instalasi *software* aplikasi yang dikembangkan bagian PPTI.
6. Melakukan pemeliharaan dan *tuning database* agar memiliki performa tinggi.
7. Melakukan pengendalian hak akses data dan informasi bagi para pengguna.
8. Melakukan proses *back up* data, aplikasi, dan perangkat lunak secara berkala dan teratur.
9. Melakukan pemilihan data dan aplikasi pemrosesannya apablia terjadi serangan dan bencana.
10. Melakukan dokumentasi aplikasi-aplikasi yang dikembangkan Bagian PPTI.
11. Memberikan masukan peningkatan atau pergantian perangkat keras dan perangkat lunak untuk menjamin berlangusungnya sistem yang lebih efektif dan lebih efisien.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

12. Melakukan evaluasi terhadap pengembangan dan penerapan teknologi informasi.
13. Mengembangkan dan memelihara situs *web* institusi beserta aplikasinya.

Tugas Pokok Seksi Media *Online*

1. Memegang seluruh *website* yang dimiliki oleh Stikom Surabaya.
2. Menjaga ketersediaan saluran *website* yang ada di Stikom Surabaya.

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA

BIODATA PENULIS

Nama : C

Nim : 1

Perguruan Tinggi : I matika Stikom Surabaya

Jurusan : S

Fakultas : T ka

Alamat : J No.64, Ambon

Tempat/Tgl Lahir : A

Agama : Islam

Email : RatuRachman@gmail.com

Riwayat Pendidikan : 2001 – 2007, MI Negeri 1 Ambon

2007 – 2010, Mts Negeri 1 Ambon

2010 – 2013, SMA Negeri 11 Ambon

2013 – 2017, Stikom Surabaya

Keorganisasian : 2013 – 2014, Anggota *Linux User Group* (LUG)

2014, Humas *Google Student Group* (GSG)

2015, Bendahara Senat Mahasiswa

2015, *Event Organizer Linux User Group* (LUG)

2016, Humas *Linux User Group* (LUG)

INSTITUT BISNIS & INFORMATIKA stikom SURABAYA